CLI GUIDE

Cisco 220 Series Smart Switches Command Line Interface Reference Guide Release 1.1.0.x

July 21, 2017

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016, 2017 Cisco Systems, Inc. All rights reserved.

Contents

Chapter 1: Introduction 23

Overview 23
User (Privilege) Levels 24
CLI Command Modes 25
User EXEC Mode 25
Privileged EXEC Mode 26
Global Configuration Mode 26
Global Configuration Submodes 27
Accessing the CLI 28
Using HyperTerminal over the Console Interface 29
Using Telnet over an Ethernet Interface 31
CLI Command Conventions 31
Editing Features 32
Entering Commands 32
Terminal Command Buffer 33
Negating the Effect of Commands 33
Command Completion 34
Keyboard Shortcuts 34
Copying and Pasting Text 34
Interface Naming Conventions 35
Interface ID 35
Interface Range 36
Interface List 36

Chapter 2: 802.1X Commands 37

dot1x guest-vlan enable 37
dot1x guest-vlan enable (Interface) 38
dot1x host-mode 39
dot1x max-hosts 40
dot1x max-req 41
dot1x port-control 42

dot1x radius-attributes vlan 43
dot1x reauthentication 44
dot1x system-auth-control 45
dot1x timeout server-timeout 45
dot1x timeout quiet-period 46
dot1x timeout reauth-period 47
dot1x timeout supp-timeout 48
dot1x timeout tx-period 49
dot1x violation-mode 50
show dot1x 51
show dot1x authenticated-hosts 53
show dot1x guest-vlan 54
show dot1x sessions 56

Chapter 3: AAA Commands 58

aaa authentication enable 58
aaa authentication login 60
enable authentication 61
enable password 62
ip http authentication 64
login authentication 65
passwords aging 66
passwords complexity <attributes> 67
passwords complexity enable 68
show aaa authentication lists 70
show line lists 70
show passwords configuration 71
show username 72
username 73

Chapter 4: ACL Commands 75

deny (MAC) 75
deny (IP) 76
deny (IPv6) 79
ip access-group in 81
ip access-list extended 82
ipv6 access-group in 83
ipv6 access-list 84
mac access-group in 85
mac access-list extended 85
no sequence 86
permit (IP) 87
permit (IPv6) 90
permit (MAC) 92
show access-lists 93
show access-lists 94
show access-lists utilization 95

Chapter 5: Address Table Commands 96

bridge multicast reserved-address 96
clear mac address-table 97
mac address-table aging-time 98
mac address-table static 98
show bridge multicast reserved-address 101
show mac address-table 102
show mac address-table aging-time 103
show port-security 104
switchport port-security 105
switchport port-security mode maximum 106

Chapter 6: Bonjour Commands 109

bonjour enable 109

show bonjour 110

Chapter 7: CDP Commands 111

cdp advertise-v2 111

cdp appliance-vlan enable 112

cdp device-id format 113

cdp enable 113

cdp holdtime 114

cdp log mismatch duplex 115

cdp log mismatch native 116

cdp log mismatch voip 117

cdp mandatory-tlvs validation 118

cdp pdu 118

cdp run 119

cdp timer 120

clear cdp counter 121

clear cdp table 122

show cdp 122

show cdp entry 123

show cdp interfaces 124

show cdp neighbors 124

show cdp tlv 126

show cdp traffic global 126

show cdp traffic (Interface) 128

Chapter 8: Clock Commands 132

absolute 132

clock set 133

clock source 134
clock summer-time 135
clock timezone 136
show time-range 137
periodic 138
show clock 139
show sntp configuration 140
sntp server 141
time-range 142

Chapter 9: Configuration and Image File Commands 144

boot host auto-config 144
boot system 145
copy 146
delete backup-config 148
delete startup-config 149
dir 149
ip dhcp tftp-server file 150
ip dhcp tftp-server ip address 151
management vlan ipv6 dhcp client information refresh 152
management vlan ipv6 dhcp client stateless 153
renew dhcp force-autoconfig 154
show backup-config 155
show boot 157
show bootvar 158
show ip dhcp tftp-server 159
show running-config 160
show startup-config 163
write 165

Chapter 10: EEE Commands 167

eee enable (Interface) 167

Chapter 11: Ethernet Configuration Commands 168

clear counters 168

clear etherlike statistics 169

default interface 169

description 170

duplex 171

errdisable recovery 171

flowcontrol 173

interface 174

interface range 175

jumbo-frame 176

operation time-range 177

show errdisable recovery 178

show interface status 179

show storm-control 180

shutdown 181

speed 182

storm-control action 184

storm-control broadcast 184

storm-control broadcast level 185

storm-control enable 186

storm-control ifg 187

storm-control unit 187

storm-control unknown-multicast 188

storm-control unknown-multicast level 189

storm-control unknown-unicast 190

storm-control unknown-unicast level 191

Chapter 12: GVRP Commands 192

clear gvrp statistics 192
gvrp enable (Global) 193
gvrp enable (Interface) 193
gvrp registration-mode 194
gvrp vlan-creation-forbid 195
show gvrp 196
show gvrp configuration 196
show gvrp error-statistics 198
show gvrp statistics 199

Chapter 13: IGMP Snooping Commands 210

clear ip igmp snooping groups 210
clear ip igmp snooping statistics 210
ip igmp filter 211
ip igmp max-groups 212
ip igmp profile 213
ip igmp snooping 214
ip igmp snooping version 215
ip igmp snooping report-suppression 215
ip igmp snooping unknown-multicast action 216
ip igmp snooping vlan 217
ip igmp snooping vlan immediate-leave 218
ip igmp snooping vlan forbidden mrouter 219
ip igmp snooping vlan forbidden forward-all 220
ip igmp snooping vlan last-member-query-count 221
ip igmp snooping vlan last-member-query-interval 221
ip igmp snooping vlan mrouter 222

ip igmp snooping vlan querier 223
ip igmp snooping vlan querier version 224
ip igmp snooping vlan query-interval 225
ip igmp snooping vlan response-time 226
ip igmp snooping vlan robustness-variable 226
ip igmp snooping vlan static 227
ip igmp snooping vlan mrouter 228
ip igmp snooping vlan forward-all 229
profile range 230
show ip igmp filter 231
show ip igmp max-group 232
show ip igmp max-group action 233
show ip igmp profile 234
show ip igmp snooping 234
show ip igmp snooping forward-all 235
show ip igmp snooping groups 236
show ip igmp snooping mrouter 237
show ip igmp snooping querier 238
show ip igmp snooping vlan 238

Chapter 14: IP Addressing Commands 240

clear arp-cache 240
ip default-gateway 240
ip domain lookup 241
ip domain name 242
ip host 243
ip name-server 244
management vlan ip-address 245
management vlan ip dhcp client 246

show arp 247
show hosts 247
show ip 248
show ip dhcp 249

Chapter 15: IP ARP Inspection Commands 250

clear ip arp inspection statistics vlan 250
ip arp inspection 250
ip arp inspection limit rate 251
ip arp inspection trust 253
ip arp inspection validate 254
ip arp inspection vlan 255
show ip arp inspection 256
show ip arp inspection interfaces 257
show ip arp inspection statistics 258

Chapter 16: IP DHCP Snooping Commands 260

clear ip dhcp snooping binding 260
clear ip dhcp snooping binding interface 260
clear ip dhcp snooping binding vlan 261
clear ip dhcp snooping database statistics 262
clear ip dhcp snooping interfaces statistics 262
ip dhcp snooping 263
ip dhcp snooping database 263
ip dhcp snooping information option 265
ip dhcp snooping information option allow-untrusted 266
ip dhcp snooping limit rate 267
ip dhcp snooping trust 268
ip dhcp snooping verify mac-address 269
ip dhcp snooping vlan 270

ip dhcp snooping vlan information option circuit-id 271
renew ip dhcp snooping database 272
show ip dhcp snooping 273
show ip dhcp snooping binding 273
show ip dhcp snooping database 274
show ip dhcp snooping information option format remote-id 275
show ip dhcp snooping interfaces 275
show ip dhcp snooping interfaces statistics 276

Chapter 17: IP Source Guard Commands 278

ip source binding 278
ip source binding max-entry 279
ip verify source 280
show ip source binding 281
show ip verify source interfaces 282

Chapter 18: IPv6 Addressing Commands 284

ipv6 default-gateway 284
management vlan ipv6-address 285
management vlan ipv6-address-autoconfig 286
management vlan ipv6-address-dhcp 287
show ipv6 288
show ipv6 dhcp 288

Chapter 19: IPv6 MLD Snooping Commands 290

clear ipv6 mld snooping groups 290
clear ipv6 mld snooping statistics 290
ipv6 mld filter 291
ipv6 mld max-groups 292
ipv6 mld profile 293

ipv6 mld snooping 294
ipv6 mld snooping report-suppression 295
ipv6 mld snooping vlan 295
ipv6 mld snooping vlan immediate-leave 296
ipv6 mld snooping vlan forbidden mrouter 297
ipv6 mld snooping vlan forbidden forward-all 298
ipv6 mld snooping vlan last-member-query-count 299
ipv6 mld snooping vlan last-member-query-interval 300
ipv6 mld snooping vlan mrouter learn pim-dvmrp 301
ipv6 mld snooping vlan query-interval 302
ipv6 mld snooping vlan response-time 303
ipv6 mld snooping vlan robustness-variable 304
ipv6 mld snooping vlan static interface 305
ipv6 mld snooping vlan mrouter 306
ipv6 mld snooping vlan forward-all 307
profile range 308
show ipv6 mld filter 309
show ipv6 mld max-group 310
show ipv6 mld max-group action 311
show ipv6 mld profile 311
show ipv6 mld snooping 312
show ipv6 mld snooping forward-all 313
show ipv6 mld snooping groups 314
show ipv6 mld snooping mrouter 315
show ipv6 mld snooping vlan 316

Chapter 20: LACP Commands 317

lacp port-priority 317
lacp system-priority 318

lacp timeout 318
show lacp 319

Chapter 21: Line Commands 325

clear line 325
exec-timeout 325
line 326
password-thresh 327
show line 328
silent-time 329
speed 329

Chapter 22: LLDP Commands 331

clear lldp statistics 331
lldp holdtime-multiplier 331
lldp lldpdu 333
lldp med 334
lldp med fast-start-repeat-count 334
lldp med location 335
lldp med network-policy voice auto 336
lldp med network-policy (Global) 337
lldp med network-policy (Interface) 339
lldp med tlv-select 340
lldp receive 340
lldp reinit 341
lldp run 342
lldp tlv-select 802.1 343
lldp tlv-select TLV 344
lldp transmit 344
lldp tx-delay 345

lldp timer 346
show lldp 347
show lldp interfaces 351
show lldp interfaces tlvs-overloading 352
show lldp local-device 353
show lldp med 354
show lldp neighbor 355
show lldp statistics 357

Chapter 23: Loopback Detection Commands 359

loopback-detection enable (Global) 359
loopback-detection enable (Interface) 360
loopback-detection interval 361
show loopback-detection 362

Chapter 24: Management ACL Commands 364

deny (Management) 364
management access-class 365
management access-list 366
no sequence (Management) 368
permit (Management) 369
show management access-class 370
show management access-list 370

Chapter 25: PHY Diagnostics Commands 372

show cable-diagnostics cable-length 372
show fiber-ports optical-transceiver 375

Chapter 26: Power over Ethernet (PoE) Commands 377

power inline 377

power inline legacy enable 378
power inline limit 379
power inline limit-mode 380
power inline priority 380
power inline traps enable 381
power inline usage-threshold 382
show env all 382
show power inline 383
show power inline consumption 385

Chapter 27: Port Channel Commands 387
channel-group 387
port-channel load-balance 388
show etherchannel summary 389

Chapter 28: Port Monitor Commands 390
monitor session destination interface 390
monitor session destination remote-span 391
monitor session source interfaces 392
monitor session source remote-span 393
no monitor session 394
remote-span 395
show monitor 396
show vlan remote-span 397

Chapter 29: QoS Commands 398
class 398
class-map 399
match 400
police 401

police aggregate 402
policy-map 403
priority-queue out num-of-queues 405
qos 406
qos advanced-mode trust 407
qos aggregate-policer 408
qos cos 410
qos map cos-queue 410
qos map dscp-queue 411
qos map precedence-queue 412
qos map queue-cos 413
qos map queue-dscp 414
qos map queue-precedence 414
qos remark 415
qos trust (Global) 416
qos trust (Interface) 417
service-policy 418
set 419
show class-map 420
show policy-map 420
show policy-map interface 421
show qos 422
show qos aggregate-policer 423
show qos interfaces 423
show qos map 424
show qos queueing 426
show rate-limit vlan 426
traffic-shape 427
trust-shape (Interface) 428

traffic-shape queue 429
trust 429
rate-limit (Interface) 431
rate-limit (VLAN) 432
wrr-queue bandwidth 433

Chapter 30: RADIUS Commands 435
radius-server default-param 435
radius-server host 436
show radius-server 438
show radius-server default-param 439

Chapter 31: RMON Commands 441
clear rmon statistics 441
rmon alarm 441
rmon event 444
rmon history 445
show rmon alarm 446
show rmon event 448
show rmon event log 449
show rmon history 450
show rmon statistics interfaces 451

Chapter 32: Security DoS Commands 455
security-suite dos (Global) 455
security-suite dos (Interface) 457
security-suite dos ip gratuitous-arps 458
show security-suite dos 459
show security-suite dos interfaces 460

Chapter 33: SNMP Commands 461

show snmp-server 461
show snmp-server community 462
show snmp-server engineid 463
show snmp-server group 464
show snmp-server host 465
show snmp-server trap 466
show snmp-server view 467
show snmp-server user 468
snmp-server 470
snmp-server community 470
snmp-server contact 472
snmp-server engineid 473
snmp-server engineid remote 473
snmp-server group 474
snmp-server host 475
snmp-server location 477
snmp-server trap 478
snmp-server user 478
snmp-server view 480

Chapter 34: STP Commands 482

clear spanning-tree detected-protocols 482
instance (MST) 483
name (MST) 484
revision (MST) 484
show spanning-tree 485
show spanning-tree interfaces 486
show spanning-tree mst 487

show spanning-tree mst configuration 488
show spanning-tree mst interfaces 489
spanning-tree 490
spanning-tree bpdu (Global) 490
spanning-tree bpdu-filter (Interface) 491
spanning-tree bpdu-guard (Interface) 492
spanning-tree cost (Interface) 493
spanning-tree forward-time 494
spanning-tree hello-time 494
spanning-tree link-type (Interface) 495
spanning-tree loopback-guard 496
spanning-tree mst port-priority 497
spanning-tree max-hops 498
spanning-tree max-age 498
spanning-tree mode 499
spanning-tree mst configuration 500
spanning-tree mst cost 501
spanning-tree mst priority 502
spanning-tree pathcost method 503
spanning-tree portfast 504
spanning-tree port-priority 504
spanning-tree priority 505
spanning-tree tx-hold-count 506

Chapter 35: SYN Protection Commands 508

security-suite syn protection mode 508
security-suite syn protection recovery 509
security-suite syn protection threshold 509
show security-suite syn protection 510

Chapter 36: Syslog Commands 512

clear logging 512
logging host 512
logging on 514
logging severity 515
show logging 516

Chapter 37: System Management Commands 519

hostname 519
ping 519
reload 521
show cpu input rate 521
show cpu utilization 522
show memory statistics 523
show services tcp-udp 524
show system languages 525
show tech-support 526
show username 529
show users 530
show version 531
port leds enable 532
show port leds configuration 533
traceroute 534

Chapter 38: TACACS+ Commands 536

show tacacs default-config 536
show tacacs 537
tacacs-server default-param 538
tacacs-server host 539

Chapter 39: Telnet and SSH Commands 541
crypto certificate generate 541
crypto key generate 542
ip ssh server 543
ip telnet server 544
Chapter 40: User Interface Commands 546
banner exec 546
banner login 547
configure 549
do 549
disable 550
end 551
enable 551
exit (Configuration) 552
exit (EXEC) 553
history 553
show banner 554
show history 555
show privilege 556
terminal length 557
Chapter 41: Voice VLAN Commands 559
show voice vlan 559
voice vlan enable 561
voice vlan aging-timeout 561
voice vlan cos 562
voice vlan cos mode 563
voice vlan dscp 564
voice vlan mode 564

voice vlan oui-table 565
voice vlan state 567
voice vlan id 568
voice vlan vpt 568

Chapter 42: VLAN Commands 570

name (vlan) 570
management-vlan 571
show interfaces protected-ports 571
show interfaces switchport 572
show management-vlan 574
show vlan 575
show vlan default-vlan 576
switchport access vlan 576
switchport default-vlan tagged 577
switchport dot1q-tunnel vlan 579
switchport forbidden default-vlan 580
switchport forbidden vlan 581
switchport general acceptable-frame-type 581
switchport general allowed vlan 582
switchport general ingress-filtering disable 584
switchport general pvid 584
switchport mode 586
switchport mode trunk uplink 587
switchport protected 588
switchport trunk allowed vlan 589
switchport trunk native vlan 590
switchport vlan tpid 591
vlan 591

vlan default-vlan 592

Chapter 43: Web Server Commands 594

ip http secure-server 594

ip http server 595

ip http timeout-policy 595

show ip http 596

show ip https 597

show services tcp-udp 598

Appendix A: Where to Go From Here 601

1

Introduction

The command-line interface (CLI) provides a text-based method for managing and monitoring the switch. You can access the command-line interface using a physical serial connection or a remote logical connection with Telnet.

This chapter describes how to use the command-line interface and contains the following topics:

- **Overview**
- **User (Privilege) Levels**
- **CLI Command Modes**
- **Accessing the CLI**
- **CLI Command Conventions**
- **Editing Features**
- **Interface Naming Conventions**

Overview

The command-line interface is divided into various modes. Each mode has a group of commands available in it. These modes are described in the **CLI Command Modes** section.

Users are assigned privilege levels. Each privilege level can access the CLI modes permitted to that level. User privilege levels are described in the **User (Privilege) Levels** section.

User (Privilege) Levels

Users may be created with one of the following user levels:

- **Level 1**—Users with this level can only run the User EXEC mode commands. Users at this level cannot access the web-based interface.
- **Level 15**—Users with this level can run all commands. Only users at this level can access the web-based interface.

A system administrator (user with level 15) can create passwords that allow a lower-level user to temporarily become a higher-level user. For example, the user may go from level 1 to 15.

Users with a lower level can raise their level by entering the **enable** command and the password for level 15. The higher level holds only for the current session.

The **disable** command returns the user to a lower level.

To create a user and assign a user level, use the **username** command. Only users with privilege level 15 can create users at this level.

Example 1—The following example creates the password for level 15 (by the administrator):

```
switchxxxxxx# configure
switchxxxxxx(config)# enable privilege 15 password level15@abc
```

Example 2—The following example creates a user with privilege level 1:

```
switchxxxxxx# configure
switchxxxxxx(config)# username john privilege 1 secret John1234
```

Example 3—The following example switches between level 1 to level 15. The user must know the password for level 15.

```
switchxxxxxx# exit
switchxxxxxx> enable 15
Password: ****** (this is the password for level 15)
switchxxxxxx#
```

NOTE If the authentication of passwords is performed on the RADIUS or TACACS+ servers, the passwords assigned to user level 15 must be configured on the external server and associated with the **$enab15$** username. See the **AAA Commands** chapter for details.

CLI Command Modes

The command-line interface is divided into four command modes. These are the command modes in the order in which they are accessed:

- **User EXEC Mode**
- **Privileged EXEC Mode**
- **Global Configuration Mode**
- **Global Configuration Submodes**

Each command mode has its own unique console prompt and set of CLI commands. Entering a question mark at the console prompt displays a list of available commands for the current mode and for the level of the user. Specific commands are used to switch from one mode to another.

Users are assigned privilege levels that determine the modes and commands available to them. User levels are described in the **User (Privilege) Levels** section.

User EXEC Mode

Users with level 1 initially log into the User EXEC mode. The User EXEC mode is used for tasks that do not change the configuration, such as performing basic tests and listing system information.

The user-level prompt consists of the switch hostname followed by a **>**. The default hostname is switchxxxxxx where xxxxxx is the last six digits of the switch's MAC address, as shown here:

```
switchxxxxxx>
```

The default hostname can be changed by using the **hostname** Global Configuration mode command.

Privileged EXEC Mode

A user with level 15 automatically logs into the Privileged EXEC mode.

The user-level prompt consists of the switch hostname followed by a **#**. The default hostname is switchxxxxxx where xxxxxx is the last six digits of the switch's MAC address, as shown here:

```
switchxxxxxx#
```

Users with level 1 can enter the Privileged EXEC mode by entering the **enable** command, and when prompted, the password for level 15.

To return from the Privileged EXEC mode to the User EXEC mode, use the **disable** command.

Global Configuration Mode

The Global Configuration mode is used to run the commands that configure the features at the system level, as opposed to the interface level.

Only users with command level 15 can access this mode.

To access the Global Configuration mode from the Privileged EXEC mode, enter the **configure** command at the Privileged EXEC mode prompt and press **Enter**. The Global Configuration mode prompt, consisting of the switch hostname followed by (config)#, is displayed:

```
switchxxxxxx(config)#
```

Use any of the following commands to return from the Global Configuration mode to the Privileged EXEC mode:

- exit
- end
- Ctrl+Z

The following example shows how to access the Global Configuration mode and return to the Privileged EXEC mode:

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# exit
switchxxxxxx#
```

Global Configuration Submodes

Various submodes may be entered from the Global Configuration mode. These submodes enable performing commands on a group of interfaces or lines, defining conditions required to allow traffic based on IPv4, IPv6, and MAC addresses, or defining the settings for management ACL, IGMP profiles, and MLD profiles.

For instance, to perform several operations on a specific interface, you can enter the Interface Configuration mode for that interface.

The following example enters the Interface Configuration mode for fa1-5 and then sets their speeds:

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# interface range gi1-5
switchxxxxxx(config-if-range)# speed 1000
switchxxxxxx(config-if-range)# exit
switchxxxxxx(config)#
```

The **exit** command returns to the Global Configuration mode.

The following submodes are available:

- **Interface**—Contains commands that configure a specific interface (port or port channel) or a range of interfaces. The **interface** Global Configuration mode command is used to enter the Interface Configuration mode.
- **Port Channel**—Contains commands used to configure port channels; for example, assigning ports to a port channel. Most of these commands are the same as the commands in the Ethernet Interface Configuration mode, and are used to manage the member ports as a single entity. The **interface Port-Channel** Global Configuration mode command is used to enter the Port Channel Interface Configuration mode.
- **IP Access-List**—Configures conditions required to allow traffic based on IP addresses. The **ip access-list** Global Configuration mode command is used to enter the IP Access-List Configuration mode.
- **IPv6 Access-List**—Configures conditions required to allow traffic based on IPv6 addresses. The **ipv6 access-list** Global Configuration mode command is used to enter the IPv6 Access-List Configuration mode.
- **Line Interface**—Contains commands used to configure the management connections for the console, Telnet, and SSH. These commands configure

connection operations such as line timeout settings. The **line** Global Configuration command is used to enter the Line Configuration mode.

- **MAC Access-List**—Configures conditions required to allow traffic based on MAC addresses. The **mac access-list** Global Configuration mode command is used to enter the MAC Access-List Configuration mode.
- **Management Access-List**—Contains commands used to define management access-lists. The **management access-list** Global Configuration mode command is used to enter the Management Access-List Configuration mode.
- **IGMP Profile**—Contains commands used to define the settings of IGMP profiles. The **ip igmp profile** Global Configuration mode command is used to enter the IGMP Profile Configuration mode.
- **MLD Profile**—Contains commands used to define the settings of MLD profiles. The **ipv6 mld profile** Global Configuration mode command is used to enter the MLD Profile Configuration mode.

To return from any Interface Configuration mode to the Global Configuration mode, use the **exit** command.

Accessing the CLI

The command-line interface can be accessed from a terminal or computer by performing one of the following tasks:

- Running a terminal application, such as HyperTerminal, on a computer that is directly connected to the switch's console port.
- Running a Telnet session from a command prompt on a computer with a network connection to the switch.
- Using SSH.

NOTE Telnet and SSH are disabled by default on the switch.

If the access is through a Telnet connection, ensure that the following conditions are met before using CLI commands:

- The switch has a defined IP address.
- Corresponding management access is granted.

- An IP path is available so that the computer and the switch can reach each other.

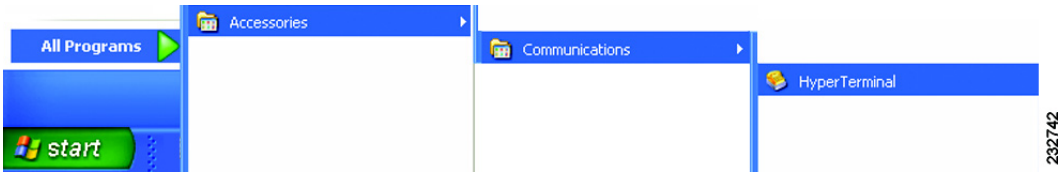
Using HyperTerminal over the Console Interface

The switch's serial console port provides a direct connection to a computer's serial port using a standard DB-9 null modem or crossover cable. Once the computer and the switch are connected, run a terminal application to access the command-line interface.

To access the command-line interface using the HyperTerminal application, perform the following steps:

STEP 1 Click the **Start** button.

STEP 2 Select **All Programs** > **Accessories** > **Communications** > **HyperTerminal**.



STEP 3 Enter a name for this connection. Select an icon for the application, then click **OK**.

STEP 4 Select a port (such as COM1) to communicate with the switch.

STEP 5 Set the serial port settings, then click **OK**.

- Bits per second = 9600
- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow control = None

STEP 6 When the command-line interface appears, enter **cisco** at the Username prompt and press **Enter**.

STEP 7 Enter **cisco** at the Password prompt and press **Enter**.

If this is the first time that you have logged on with the default username and password, or the switch has been rebooted to factory defaults, you are asked to change your password. The following message appears:

```
Please change your password from the default settings. Please change the
password for better protection of your network. Do you want to change the
password (Y/N) [Y]?
```

STEP 8 Enter **Y**, and set a new administrator password.

Password complexity is enabled on the switch by default. Passwords must conform to the following default settings:

- Have a minimum length of eight characters.
- Contain characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Are different from the current password.
- Contain no character that is repeated more than three times consecutively.

STEP 9 Press **Enter**.

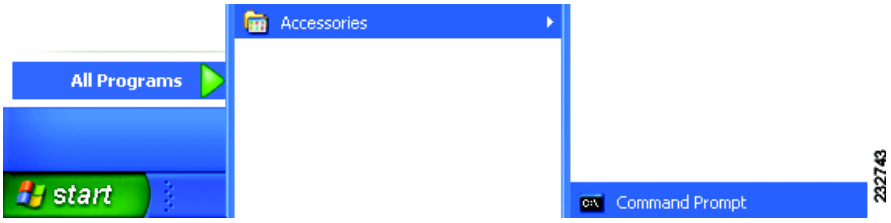
The switchxxxxxx# prompt is displayed. You can now enter the commands to manage the switch. For detailed information about the commands, refer to the appropriate chapters of this reference guide.

Using Telnet over an Ethernet Interface

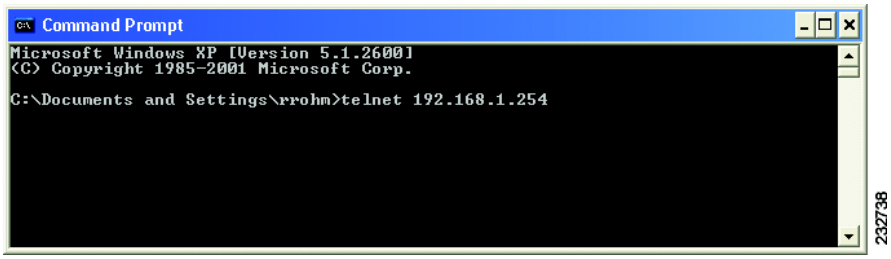
Telnet provides a method of connecting to the command-line interface over an IP network.

To establish a Telnet session from the command prompt, perform the following steps:

STEP 1 Click **Start**, then select **All Programs** > **Accessories** > **Command Prompt** to open a command prompt.



STEP 2 At the prompt, enter **telnet <IP address of switch>**, then press **Enter**.



The command-line interface is displayed.

CLI Command Conventions

There are certain command entry standards that apply to all commands. The following table describes the command conventions:

[ ]	In a command line, square brackets indicate an optional entry.

{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated with the | character. One option must be selected. For example, **flowcontrol** {**auto** | **on** | **off**} means that for the **flowcontrol** command, either **auto**, **on**, or **off** must be selected.
parameter	Italic text indicates a parameter.
bold	Command names and keywords are shown in **bold**.
italics	Variables and arguments are shown in *italics*.
press **key**	Names of keys to be pressed are shown in **bold**.
Ctrl+F4	Keys separated by the + character are to be pressed simultaneously on the keyboard.
`Screen Display`	Fixed-width font indicates CLI prompts, CLI commands entered by the user, and system messages displayed on the console.

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** *gi1*, **show**, **interfaces**, and **status** are keywords, *gi* is an argument that specifies the interface type, and *1* specifies the port.

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

```
switchxxxxxx(config)# username admin secret Nn148279
```

When working with the CLI, the command options are not displayed. The standard command to request help is **?**.

There are two instances where 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**—If a command is incomplete and the character **?** is entered in place of a parameter, the matched keyword or parameters for this command are displayed.

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.

Up-Arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-Arrow key	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.

By default, the history buffer system is enabled, but it can be disabled at any time. For more information on enabling or disabling the history buffer, refer to the **history** command.

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. For more information on configuring the command history buffer, refer to the **history** command.

To display the history buffer, refer to the **show history** command.

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 reference guide provides a description of the negation effect for each CLI command.

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 **Tab** after an incomplete command is entered, the system will attempt to identify and complete the command. 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.

Keyboard Shortcuts

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

Up-arrow	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow	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.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.
Backspace	Deletes one character left to the cursor position.

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device.

NOTE It is the user's responsibility to ensure that the text copied into the device consists of legal commands only.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.
- The commands contain no encrypted data, such as encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device except for encrypted passwords where the keyword encrypted is used before the encrypted data.

Interface Naming Conventions

Interface ID

Within the command-line interface, the interfaces are denoted by concatenating the following elements:

- **Type of interface—**The following types of interfaces are found on the various types of devices:
  - **Fast Ethernet (10/100 bits)—**This can be written as **FastEthernet** or **fa**.
  - **Gigabit Ethernet ports (10/100/1000 bits)—**This can be written either **GigabitEthernet** or **gi**.
  - **LAG (Port Channel)—**This can be written as either **Port-Channel** or **po**.
- **Interface Number—**Port, LAG, tunnel, or VLAN ID.

The syntax for this is:

```
{<port-type>[ ]<port-number>}|{Port-Channel|po}[ ]<port-channel-number>
```

Sample of these various options are shown in the example below:

```
switchxxxxxx# configure
switchxxxxxx(config)# interface gi1
switchxxxxxx(config)# interface fa1
switchxxxxxx(config)# interface Port-Channel 1
switchxxxxxx(config-if)#
```

Interface Range

Interfaces may be described on an individual basis or within a range. The interface range command has the following syntax:

```
<interface-range> ::=
{<port-type>[ ][<first-port-number>[ - <last-port-number]}|
{Port-Channel|po}[ ]<first-port-channel-number>[ - <last-port-channel-
number>]
```

A sample of this command is shown in the example below:

```
switchxxxxxx# configure
switchxxxxxx(config)# interface range gi1-5
switchxxxxxx(config-if-range)#
```

Interface List

A combination of interface types can be specified in the **interface range** command in the following format:

```
<range-list> ::= <interface-range> | <range-list>,< interface-range>
```

NOTE Range lists can contain either ports or port channels. The space after the comma is optional. When a range list is defined, a space after the first entry and before the comma (,) must be entered.

A sample of this command is shown in this example:

```
switchxxxxxx# configure
switchxxxxxx(config)# interface range gi1,gi4-5
switchxxxxxx(config-if-range)#
```

2

802.1X Commands

dot1x guest-vlan enable

To enable the guest VLAN feature on the switch and specify a VLAN as the guest VLAN, use the **dot1x guest-vlan enable** Global Configuration mode command.

To disable the guest VLAN feature on the switch, use the **no** form of this command.

Syntax

dot1x guest-vlan *vlan-id* **enable**

no dot1x guest-vlan enable

Parameters

- *vlan-id* —Identifier of the VLAN set as the guest VLAN.

Default Configuration

Guest VLAN is disabled on the switch.

Command Mode

Global Configuration mode

User Guidelines

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the interface automatically joins the guest VLAN when the interface is unauthorized and leaves it when the interface becomes authorized. To be able to join or leave the guest VLAN, the interface should not be a static member of the guest VLAN.

Example

The following example sets VLAN 2 as the guest VLAN:

```
switchxxxxxx(config)# dot1x guest-vlan 2 enable
```

dot1x guest-vlan enable (Interface)

To enable unauthorized users on the interface accessing the guest VLAN, use the **dot1x guest-vlan enable** Interface Configuration (Ethernet) mode command.

To disable unauthorized users on the interface accessing the guest VLAN, use the **no** form of this command.

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Parameters

N/A

Default Configuration

Unauthorized users cannot access the guest VLAN by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The switch can have only one guest VLAN. The guest VLAN is defined in the **dot1x guest-vlan enable** Global Configuration mode command.

Example

The following example enables unauthorized users on gi15 to access the guest VLAN:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

dot1x host-mode

To allow a single host (client) or multiple hosts on an IEEE 802.1X-authorized port, use the **dot1x host-mode** Interface Configuration mode command.

To restore the default setting, use the **no** form of this command.

Syntax

dot1x host-mode {**multi-host** | **single-host** | **multi-sessions**}

no dot1x host-mode

Parameters

- **multi-host**—Enable multiple-host mode.
- **single-host**—Enable single-host mode.
- **multi-sessions**—Enable multiple-sessions mode.

Default Configuration

Default mode is multi-host.

Command Mode

Interface Configuration mode

User Guidelines

In multiple hosts 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.

In multiple sessions mode each host must be successfully authorized in order to grant network access. Please note that packets are NOT encrypted, and after success full authentication filtering is based on the source MAC address only.

It is recommended to enable reauthentication when working in multiple-sessions mode in order to detect user logout for users that have not logged off.

In single host mode there is only one attached host and only this authenticated host can access the network.

Example

The following example sets the host mode:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x host-mode multi-host
switchxxxxxx(config-if)# dot1x host-mode single-host
switchxxxxxx(config-if)# dot1x host-mode multi-sessions
```

dot1x max-hosts

To set the maximum authenticated hosts allowed, use the **dot1x max-hosts** Interface Configuration mode command.

To restore the default value, use the **no** form of this command.

Syntax

dot1x max-hosts *number*

no dot1x max-hosts

Parameters

- **max-hosts** *number*—Maximum allowed authenticated hosts number. (Range: 1–256.)

Default Configuration

The default maximum host number is 256

Command Mode

Interface Configuration mode

User Guidelines

The command is relevant only for multi-sessions mode.

Example

The following example sets the maximum host number to 5:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x max-hosts 5
```

dot1x max-req

To set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) request or identity frame (assuming that no response is received) to the client before restarting the authentication process, use the **dot1x max-req** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

- *count*—The maximum number of times that the switch sends an EAP request or identity frame before restarting the authentication process. (Range: 1 to 10)

Default Configuration

The default maximum number of attempts is 2.

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.

Example

The following example sets the maximum number of EAP requests to 6:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x max-req 6
```

dot1x port-control

To enable manual control of the port authorization state, use the **dot1x port-control** Interface Configuration (Ethernet) mode command.

To disable manual control of the port authorization state, use the **no** form of this command.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

Parameters

- **auto**—Enables 802.1X authentication on the interface and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the switch and the client.
- **force-authorized**—Disables 802.1X authentication on the interface and causes the interface to transition to the authorized state without any authentication exchange required. The interface resends and receives normal traffic without 802.1X-based client authentication.
- **force-unauthorized**—Denies all access through this interface by forcing it to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through this interface.

Default Configuration

The interface is in the force-authorized state.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

In order to proceed to the forwarding state immediately after successful authentication, we recommend that you disable STP or enable the STP PortFast mode on 802.1X edge ports (ports in auto state that are connected to end stations).

Example

The following example enables 802.1X authentication in auto mode on gi15:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x port-control auto
```

dot1x radius-attributes vlan

To enable user-based VLAN assignment, use the **dot1x radius-attributes vlan** Interface Configuration mode command.

To disable user-based VLAN assignment, use the **no** form of this command.

Syntax

dot1x radius-attribute vlan {**reject** | **static**}

no dot1x radius-attribute vlan

Parameters

- **reject**—If the RADIUS server authenticated the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected.
- **static**—If the RADIUS server authenticated the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.

Default Configuration

Disabled

Command Mode

Interface Configuration mode

User Guidelines

When RADIUS attributes are enabled and the RADIUS accept message does not contain the supplicant's VLAN as an attribute, the supplicant is rejected in reject mode.

Packets to the supplicant are sent untagged.

After successful authentication, the port remains a member in the guest VLAN.

Example

The following example sets VLAN assign mode to reject:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x radius-attributes vlan reject
```

dot1x reauthentication

To enable periodic reauthentication of the client, use the **dot1x reauthentication** Interface Configuration (Ethernet) mode command.

To disable periodic reauthentication of the client, use the **no** form of this command.

Syntax

dot1x reauthentication

no dot1x reauthentication

Parameters

N/A

Default Configuration

Periodic reauthentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x reauthentication
```

dot1x system-auth-control

To enable 802.1X globally on the switch, use the **dot1x system-auth-control** Global Configuration mode command.

To disable 802.1X globally on the switch, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Parameters

N/A

Default Configuration

802.1X is disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# dot1x system-auth-control
```

dot1x timeout server-timeout

To set the time interval during which the device waits for a response from the authentication server, use the **dot1x timeout server-timeout** Interface Configuration mode command.

To restore the default server timeout, use the **no** form of this command.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

- **server-timeout** *seconds*—Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds.)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration mode

User Guidelines

The actual timeout period can be determined by comparing the value specified by the dot1x timeout server-timeout command to the result of multiplying the number of retries specified by the radius-server retransmit command by the timeout period specified by the radius-server retransmit command, and selecting the lower of the two values.

Example

The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

dot1x timeout quiet-period

To set the time interval that the switch remains in a quiet state following a failed authentication exchange (for example, the client provided an invalid password), use the **dot1x timeout quiet-period** Interface Configuration (Ethernet) mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters

- *seconds*—The time interval in seconds that the switch remains in a quiet state following a failed authentication exchange with the client. (Range: 0 to 65535 seconds)

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the switch does not accept or initiate the authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

Example

The following example sets the time interval to 10 seconds:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x timeout quiet-period 10
```

dot1x timeout reauth-period

To set the number of seconds between reauthentication attempts, use the **dot1x timeout reauth-period** Interface Configuration (Ethernet) mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

dot1x timeout reauth-period *seconds*

no dot1x timeout reauth-period

Parameters

- *seconds*—Number of seconds between reauthentication attempts. (Range: 30 to 65535)

Default Configuration

3600 seconds

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

dot1x timeout supp-timeout

To set the time interval during which the switch waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request, use the **dot1x timeout supp-timeout** Interface Configuration (Ethernet) mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

- *seconds*—The time interval in seconds during which the switch waits for a response to an EAP request frame from the client before resending the request. (Range: 1 to 65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

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.

Example

The following example sets the time interval to 3600 seconds:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout tx-period

To set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request, use the **dot1x timeout tx-period Interface** Configuration (Ethernet) mode command.

To restore the default tx period, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters

- **tx-period** *seconds*—Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 30–65535 seconds.)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration 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.

Example

The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 60 seconds:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

dot1x violation-mode

To configure the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface, use the **dot1x violation-mode** Interface Configuration mode command.

To restore the default, use the **no** form of this command.

Syntax

dot1x violation-mode {**restrict** | **protect** | **shutdown**} [**trap** *seconds*]

no dot1x violation-mode

Parameters

- **restrict**—Generates a trap when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. Those frames are forwarded but their source addresses are not learned.
- **protect**—Discard frames with source addresses not the supplicant address.
- **shutdown**—Discard frames with source addresses not the supplicant address and shutdown the port.
- **trap** *seconds*—Send SNMP traps, and specifies the minimum time between consecutive traps. If seconds = 0, traps are disabled.

Default Configuration

Protect.

Command Mode

Interface Configuration mode

User Guidelines

The command is relevant only for single-host mode.

Example

The following command sets the single host violation mode to restrict with trap frequency 10 seconds:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x violation-mode restrict trap 10
```

show dot1x

To display the 802.1X global or specified interface status, use the **show dot1x** Privileged EXEC mode command.

Syntax

show dot1x [**interfaces** *interface-id*]

Parameters

- **interface-id**—Specify port list

Default Configuration

Display for all ports.

Command Mode

Privileged EXEC mode

Example

Example 1—The following example shows 802.1X status on port gi1:

```
switchxxxxxx#show dot1x interfaces gi1
Interface Configurations

Interface FastEthernet2
  Admin Control          : disabled
  Host Mode              : single-host
  Guest VLAN             : disabled
  RADIUS VLAN Assign     : disable
  Single-host Violation  : restrict
    Trap Frequency       : 3
    Violation Detected   : 0
  Reauthentication       : enabled
  Reauthenticate Period  : 3600
  Max Hosts              : 256
  Quiet Period           : 60
  EAP Max Request        : 2
  EAP TX Period          : 30
  Supplicant Timeout     : 30
  Server Timeout         : 30
```

Example 2—The following example shows all 802.1X statuses:

```
switchxxxxxx#show dot1x
Authentication dot1x state     : enabled
Guest VLAN                    : enabled (3)

Interface Configurations

Interface FastEthernet1
  Admin Control          : auto
  Host Mode              : multi-host
  Guest VLAN             : disabled
  RADIUS VLAN Assign     : disable
  Reauthentication       : enabled
  Reauthenticate Period  : 3600
  Max Hosts              : 256
  Quiet Period           : 60
  EAP Max Request        : 2
  EAP TX Period          : 30
  Supplicant Timeout     : 30
  Server Timeout         : 30

Interface FastEthernet2
  Admin Control          : disabled
  Host Mode              : single-host
  Guest VLAN             : disabled
  RADIUS VLAN Assign     : disable
  Single-host Violation  : restrict
    Trap Frequency       : 3
    Violation Detected   : 0
  Reauthentication       : enabled
  Reauthenticate Period  : 3600
```

```
  Max Hosts               : 256
  Quiet Period            : 60
  EAP Max Request         : 2
  EAP TX Period           : 30
  Supplicant Timeout      : 30
  Server Timeout          : 30
.....
```

show dot1x authenticated-hosts

To show information for all dot1x authenticated hosts, use the **show dot1x authenticated-hosts** Privileged EXEC mode command.

Syntax

show dot1x authenticated-hosts

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following command shows all authenticated hosts:

```
switchxxxxxx# show dot1x authenticated-hosts
Interface  MAC Address       Session Time   VLAN ID  User Name
---------- ----------------- -------------- -------- ----------------------
```

The following table describes the significant fields shown in the example:

Field	Description
Interface	Port number.
MAC Address	Supplicant MAC address.

Field	Description
Session Time	Amount of time that the supplicant was logged on the port.
VLAN ID	Supplicant VLAN ID.
User Name	Supplicant name that was authenticated on the port.

show dot1x guest-vlan

To show the 802.1X guest VLAN information for all interfaces, use the **show dot1x guest-vlan** Privileged EXEC mode command.

Syntax

show dot1x guest-vlan

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show dot1x guest-vlan
 Guest VLAN ID: none (disabled)

  Port   | Guest VLAN | In Guest VLAN
--------+------------+---------------
   gi1   |   Enabled  |       No
   gi2   |   Disabled |       ---
   gi3   |   Disabled |       ---
   gi4   |   Disabled |       ---
   gi5   |   Disabled |       ---
   gi6   |   Disabled |       ---
   gi7   |   Disabled |       ---
   gi8   |   Disabled |       ---
   gi9   |   Disabled |       ---
  gi10   |   Disabled |       ---
```

```
gi11   |   Disabled |       ---
gi12   |   Disabled |       ---
gi13   |   Disabled |       ---
gi14   |   Disabled |       ---
gi15   |   Enabled  |       No
gi16   |   Disabled |       ---
gi17   |   Disabled |       ---
gi18   |   Disabled |       ---
gi19   |   Disabled |       ---
gi20   |   Disabled |       ---
gi21   |   Disabled |       ---
gi22   |   Disabled |       ---
gi23   |   Disabled |       ---
gi24   |   Disabled |       ---
gi25   |   Disabled |       ---
gi26   |   Disabled |       ---
gi27   |   Disabled |       ---
gi28   |   Disabled |       ---
gi29   |   Disabled |       ---
gi30   |   Disabled |       ---
gi31   |   Disabled |       ---
gi32   |   Disabled |       ---
gi33   |   Disabled |       ---
gi34   |   Disabled |       ---
gi35   |   Disabled |       ---
gi36   |   Disabled |       ---
gi37   |   Disabled |       ---
gi38   |   Disabled |       ---
gi39   |   Disabled |       ---
gi40   |   Disabled |       ---
gi41   |   Disabled |       ---
gi42   |   Disabled |       ---
gi43   |   Disabled |       ---
gi44   |   Disabled |       ---
gi45   |   Disabled |       ---
gi46   |   Disabled |       ---
gi47   |   Disabled |       ---
gi48   |   Disabled |       ---
gi49   |   Disabled |       ---
gi50   |   Disabled |       ---
gi51   |   Disabled |       ---
gi52   |   Disabled |       ---
```

The following table describes the significant fields shown in the example:

Field	Description
Guest VLAN ID	Identifier of the VLAN as the guest VLAN.
Port	Port number.

Field	Description
Guest VLAN	Shows whether 802.1X authentication is enabled or disabled on the port.
In Guest VLAN	Shows whether the unauthorized port is in or not in the guest VLAN.

show dot1x sessions

To display the 802.1X authentication sessions information, use the **show dot1x sessions** Privileged EXEC mode command.

Syntax

show dot1x sessions [{**detail** | **interfaces** *interface-id* | **session-id** *session-id*}]

Parameters

- **detail**—Display detail information of all sessions.
- **interfaces** *interface-id*—Display detail information of session on specific interface
- **session-id** *session-id*—Display detail information of session with specific session id

Default Configuration

Display brief information of all sessions

Command Mode

Privileged EXEC mode

Example

Example 1—The following example shows 802.1X brief session information:

```
Switchxxxxxx#show dot1x sessions
Total Session Number: 1

Interface  MAC Address       Authenticator State    Status       Session ID
---------- ----------------- ---------------------- ------------ ------------
```

```
fa7        68:BD:AB:A5:89:D4 Authorized            Authorized
00000010017DB6C0
```

The following table describes the significant fields shown in the example:

Field	Description
Interface	The interface name of the session.
MAC Address	Supplicant MAC address.
Authenticator State	802.1X PAE authenticator state
Status	Running—Authentication is ongoing Authorized—Authentication success UnAuthorized—Authentication fail Locked—Supplicant is in quiet period
Session ID	Unique authentication session ID.

Example 2—The following shows 802.1X detail session information:

```
Switchxxxxxx#show dot1x sessions detail
Interface               : FastEthernet7
MAC Address             : 68:BD:AB:A5:89:D4
Session ID              : 00000010017DB6C0
Authenticator State     : Authorized
User Name               : CP-7975G-SEP68BDABA589D4
Authorized Information
  VLAN                  : N/A
  Reauthenticate Period: 300 (from RADIUS)
Operational Information
  VLAN                  : 1
  Session Time          : 182
```

3

AAA Commands

This chapter describes the Authentication, Authorization, and Accounting (AAA) commands.

aaa authentication enable

To set one or more authentication methods for accessing higher privilege levels, use the **aaa authentication enable** Global Configuration mode command.

To restore the default authentication method, use the **no** form of this command.

Syntax

aaa authentication enable {**default** | *LISTNAME*} *method1* [*method2* ...]

no aaa authentication enable {**default** | *LISTNAME*}

Parameters

- **default**—Uses the default authentication method list when accessing higher privilege levels.
- *LISTNAME* —Name of the authentication method list activated when users access higher privilege levels. (Length: 1 to 32 characters)
- *method1* [*method2* ...]—A list of methods that the authentication algorithm tries, in the given sequence.

Default Configuration

The **enable password** command defines the default authentication login method. This command functions the same as the **aaa authentication enable default enable** command.

On a console, the **enable password** is used if a password exists. If no password is set, the authentication still succeeds. This command functions the same as entering the **aaa authentication enable default enable none** command.

Command Mode

Global Configuration mode

User Guidelines

A user who logs on with a lower privilege level must pass these authentication methods to access a higher level.

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

Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
none	Uses no authentication.
radius	Uses a list of RADIUS servers for authentication.
tacacs+	Uses a list of TACACS servers for authentication.

Create a list by entering the **aaa authentication enable** *LISTNAME* command where *LISTNAME* 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.

All **aaa authentication enable default** requests sent by the switch to a RADIUS or a TACACS+ server include the username **$enabx$.**, where **x** is the requested privilege level.

The **no aaa authentication enable** *LISTNAME* command deletes the list name if it has not been referenced.

Example

The following example sets the enable password for authentication for accessing higher privilege levels:

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

aaa authentication login

To set one or more authentication methods to be applied during login, use the **aaa authentication login** Global Configuration mode command.

To restore the default authentication method, use the **no** form of this command.

Syntax

aaa authentication login {**default** | *LISTNAME*} *method1 [method2...]*

no aaa authentication login {**default** | *LISTNAME*}

Parameters

- **default**—Uses the default authentication method list when a user logs in (this list is unnamed).
- *LISTNAME*—Name of the authentication method list activated when a user logs in. (Length: 1 to 32 characters)
- *method1 [method2...]*—A list of methods that the authentication algorithm tries (in the given sequence).

Default Configuration

If no authentication method is specified, the default is to use the locally-defined users and passwords. It is the same as entering the **aaa authentication login local** command.

NOTE If no authentication method is defined, the console users can log in without any authentication verification.

Command Mode

Global Configuration mode

User Guidelines

A list of authentication methods may be assigned a list name, and this list name can be used in the **aaa authentication enable** command.

Create a list of authentication methods by entering this command with the *LISTNAME* parameter where *LISTNAME* is any character string. The method argument identifies the list of methods that the authentication algorithm tries in the given sequence.

Each additional authentication method is 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.

Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
local	Uses the locally defined usernames for authentication.
none	Uses no authentication.
radius	Uses a list of RADIUS servers for authentication.
tacacs+	Uses a list of TACACS+ servers for authentication.

The default and list names created with this command are used with the **aaa authentication enable** command.

The **no aaa authentication login** *LISTNAME* command deletes a list name only if it has not been referenced by another command.

Example

The following example sets the authentication login method for console sessions:

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

enable authentication

To specify the authentication method for accessing a higher privilege level from a remote Telnet or console, use the **enable authentication** Line Configuration mode command.

To restore the default authentication method, use the **no** form of this command.

Syntax

enable authentication *LISTNAME*

no enable authentication

Parameters

- *LISTNAME*—Name of a specific authentication method list created with the **aaa authentication enable** command.

Command Mode

Line Configuration mode

Examples

Example 1—The following example uses the default authentication method when accessing a higher privilege level from a console:

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

Example 2—The following example sets a list of authentication methods for accessing higher privilege levels:

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

enable password

To set a local password to control access to normal and privilege levels, use the **enable password** Global Configuration mode command.

To restore the default password, use the **no** form of this command.

Syntax

enable password [**level** *privilege-level*] *unencrypted-password*

enable secret [**level** *privilege-level*] **encrypted** *encrypted-password*

no enable [**password** | **secret**] [**level** *privilege-level*]

Parameters

- **level** *privilege-level*—(Optional) Specifies the level for which the password applies. If not specified, the level is 15. (Range: 1 to 15)
- *unencrypted-password*—Password for this level. (Range: 0 to 80 characters)
- *encrypted-password*—The encrypted password. Use this keyword to enter a password that is already encrypted, such as a password that you copied from the configuration file of another device.

Default Configuration

The default level is 15.

The passwords are encrypted by default.

Command Mode

Global Configuration mode

User Guidelines

When the administrator configures a new **enable** password, this password is encrypted automatically and saved to the configuration file. No matter how the password was entered, it appears in the configuration file with the keyword **encrypted** and the encrypted value.

If the administrator wants to manually copy a password that was configured on one switch (switch B) to another switch (switch A), the administrator must add **encrypted** in front of this encrypted password when entering the **enable** command in switch A. In this way, the two switches will have the same password.

The passwords are encrypted by default. You only are required to use the **encrypted** keyword when you are actually entering an encrypted keyword.

Example

The following command sets an unencrypted password for level 15 (it will be encrypted in the configuration file):

```
switchxxxxxx(config)# enable password level 15 let-me-in
switchxxxxxx(config)# enable secret level 1
4b529f21c93d4706090285b0c10172eb073ffebc4
```

ip http authentication

To specify one or more AAA methods for HTTP and HTTPS login authentications, use the **ip http authentication** Global Configuration mode command.

Syntax

ip http authentication aaa login-authentication [**http** | **https**] {**default** | *LISTNAME*}

no ip http authentication aaa login-authentication [**http** | **https**]

Parameters

- **http**—(Optional) Binds a login authentication list to user access with the HTTP protocol.
- **https—**(Optional) Binds a login authentication list to user access with the HTTPS protocol.
- **default—**Uses the default login authentication method list.
- *LISTNAME*—Name of the login authentication method list.

Default Configuration

The default login authentication list is used for HTTP and HTTPS sessions by default.

Command Mode

Global Configuration mode

Example

The following example creates two login authentication method lists and binds them to HTTP and HTTPS separately:

```
switchxxxxxx(config)# ip http authentication aaa login-authentication http
test1
switchxxxxxx(config)# ip http authentication aaa login-authentication https
test2
```

login authentication

To specify the login authentication method list for a remote Telnet or console session, use the **login authentication** Line Configuration mode command.

To restore the default authentication method, use the **no** form of this command.

Syntax

login authentication {**default** | *LISTNAME*}

no login authentication

Parameters

- **default**—Uses the default login authentication list.
- *LISTNAME*—Name of a specific authentication list created with the **aaa authentication login** command.

Default Configuration

The default login authentication list is used for each line.

Command Mode

Line Configuration mode

Examples

Example 1—The following example specifies the default login authentication method for a console session:

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

Example 2—The following example sets an authentication login method list for the console:

```
switchxxxxxx (config)# aaa authentication login authen-list radius local none
switchxxxxxx (config)# line console
switchxxxxxx (config-line)# login authentication authen-list
```

passwords aging

To enforce the password aging, use the **passwords aging** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

passwords aging *days*

no passwords aging

Parameters

- *days*—The number of days before a password change is forced. The value of zero means disabling aging. (Range: 0 to 365)

Default Configuration

The number of days is 180.

Command Mode

Global Configuration mode

User Guidelines

Aging is relevant only to local users with the privilege level 15.

To disable the password aging, use **passwords aging 0**. Using **no passwords aging** restores the aging time to its default setting.

Example

The following example configures the aging time to 24 days:

```
switchxxxxxx(config)# passwords aging 24
```

passwords complexity <attributes>

To configure the minimum password requirements when the password complexity is enabled, use the **passwords complexity <attributes>** Global Configuration mode commands.

To revert to its default setting, use the **no** form of these commands.

Syntax

passwords complexity min-length *number*

no passwords complexity min-length

passwords complexity min-classes *number*

no passwords complexity min-classes

passwords complexity not-current

no passwords complexity not-current

passwords complexity no-repeat *number*

no password complexity no-repeat

passwords complexity not-username

no passwords complexity not-username

Parameters

- **min-length** *number*—Specifies the minimum length of the password. (Range: 0 to 64 characters)
- **min-classes** *number*—Specifies the minimum character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 0 to 4)
- **not-current**—Specifies that the new password cannot be same as the current password.
- **no-repeat** *number*—Specifies the maximum number of characters that can be repeated consecutively. Zero specifies that there is no limit on repeated characters. (Range: 0 to 16)
- **not-username**—Specifies that the new password cannot be same as the current username.

Default Configuration

The minimum length is 8.

The number of classes is 3.

The default for no-repeat is 3.

All other controls are enabled by default.

Command Mode

Global Configuration mode

Example

The following example changes the minimum required password length to 10 characters:

```
switchxxxxxx(config)# passwords complexity min-length 10
```

passwords complexity enable

To enforce the minimum password complexity, use the **passwords complexity enable** Global Configuration mode command.

To disable enforcing the password complexity, use the **no** form of this command.

Syntax

passwords complexity enable

no passwords complexity enable

Parameters

N/A

Default Configuration

Password complexity is enabled on the switch.

Command Mode

Global Configuration mode

User Guidelines

The password complexity is enabled by default. The user is required to enter a password that:

- Has a minimum length of 8 characters.
- Contains characters from at least 3 character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Is different from the current password.
- Contains no character that is repeated more than 3 times consecutively.

You can control these attributes of the password complexity with specific commands described in this section.

If you have previously configured other complexity settings, then those settings are used. This command does not eliminate the other settings. It works only as a toggle.

Example

The following example enables enforcing the password complexity on the switch and shows the current password complexity settings:

```
switchxxxxxx(config)# passwords complexity enable
switchxxxxxx(config)# exit
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
```

show aaa authentication lists

To show information for the AAA authentication lists, use the **show aaa authentication lists** Privileged EXEC command.

Syntax

show aaa authentication {**login** | **enable**} **lists**

Parameters

- **login**—Displays information for the AAA authentication login lists.
- **enable**—Displays information for the AAA authentication enable lists.

Command Mode

Privileged EXEC mode

Example

The following examples show information for all existing login and enable authentication lists:

```
switchxxxxxx# show aaa authentication login lists
 Login List Name   | Authentication Method List
-----------------+--------------------------------
          default   |  local

switchxxxxxx# show aaa authentication enable lists
 Enable List Name   | Authentication Method List
-----------------+--------------------------------
          default   |  enable
```

show line lists

To show all AAA method lists for different line types, use the **show line lists** Privileged EXEC mode command.

Syntax

show line lists

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays all AAA method lists for different line types:

```
switchxxxxxxx# show line lists
Line Type   |    AAA Type      |  List Name
------------+------------------+-----------------
     console |           login | default
             |          enable | default
      telnet |           login | default
             |          enable | default
         ssh |           login | default
             |          enable | default
        http |           login | default
       https |           login | default
```

show passwords configuration

To show the password management configuration, use the **show passwords configuration** Privileged EXEC mode command.

Syntax

show passwords configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
```

show username

To show all user accounts in local database, use the **show username** Privileged EXEC mode command.

Syntax

show username

Parameters

None

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example shows information for all user accounts defined on the switch:

```
switchxxxxxx# show username
Priv   |  Type   |            User Name             |             Password
-------+--------+----------------------------------+--------------------------
```

```
  15    | secret |                          cisco |
ZmZmNzVhZTAzYjAyODkzZjlkM2JjZGIyMGYyMzY0NDM=
```

username

To add a new user or edit an existing user, use the **username** Global Configuration mode command.

To delete a username, use the **no** form of this command.

Syntax

username *USERNAME* [**privilege** {**1** | **15** | **admin** | **user**}] {**nopassword** | **secret** {**Encrypted** *encrypted-password* | *unencrypted-password*}}

no username *USERNAME*

Parameters

- *USERNAME*—Name of the user. (Range: 0 to 32 characters)
- **privilege 1** —(Optional) Specifies the privilege level to 1.
- **privilege 15** —(Optional) Specifies the privilege level to 15.
- **privilege admin** —(Optional) Specifies the privilege level to 15.
- **privilege user** —(Optional) Specifies the privilege level to 1.
- **nopassword**—No password is required for this user to log in.
- **secret Encrypted** *encrypted-password*—Specifies an encrypted password for the user. Use this keyword to enter a password that is already encrypted, such as a password that you copied from another the configuration file of another device.
- **secret** *unencrypted-password*—Specifies a password that will be automatically encrypted. (Range: 0 to 80 characters)

Default Configuration

The privilege level of the default user **cisco** is 15. The default password of this user is **cisco**.

Command Mode

Global Configuration mode

Examples

Example 1—The following example adds a user tom (level 15) with no password:

```
switchxxxxxx(config)# username tom privilege 15 nopassword
```

Example 2—The following example sets a password for user jerry (level 15) that has already been encrypted. It will be copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# username jerry privilege 15 secret encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

4

ACL Commands

deny (MAC)

To set deny conditions (conditions are also known as access control entries [ACEs]) for a MAC-based ACL, use the **deny** MAC Access-List Configuration mode command.

To remove a MAC-based ACE, use the **no sequence** command.

Syntax

deny {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**vlan** *vlan-id*] [**cos** *cos cos-wildcard*] [**ethtype** *value*] [**disable-port**]

no sequence *value*

Parameters

- **any**—Any source or destination MAC address of the packet.
- *source*—Source MAC address of the packet.
- *source-wildcard*—Wildcard bits to be applied to the source MAC address.
- *destination*—Destination MAC address of the packet.
- *destination-wildcard*—Wildcard bits to be applied to the destination MAC address.
- **vlan** *vlan-id*—(Optional) Specifies the VLAN ID of the packet. (Range: 1 to 4094)
- **cos** *cos*—(Optional) Specifies the CoS value of the packet. (Range: 0 to 7)
- *cos-wildcard*—(Optional) Wildcard bits to be applied to the CoS value.
- **ethtype** *value*—(Optional) Specifies the Ethernet type in hexadecimal format of the packet.

- **disable-port—**(Optional) Disables the Ethernet interface if the condition is matched.

Default Configuration

No MAC-based ACE is defined.

Command Mode

MAC Access-List Configuration mode

User Guidelines

After an ACE is added to an ACL, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-acl)# deny 00:00:00:00:00:01 00:00:00:00:00:ff any
```

deny (IP)

To set deny conditions for an IPv4-based ACL, use the **deny** IP Access-List Configuration mode command.

To remove an IPv4-based ACE, use the **no sequence** command.

Syntax

[**sequence** *value*] **deny** *protocol* {**any** | *source source-wildcard* } {**any** | *destination destination-wildcard*} [**dscp** *number* | **precedence** *number*] [**disable-port**]

[**sequence** *value*] **deny** *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard* } [**any** | *icmp-type*] [**any** | *icmp-code*] [**dscp** *number* | **precedence** *number*] [**disable-port**]

[**sequence** *value*] **deny** *tcp* {**any** | {*source source-wildcard*} {**any** | *source-port*/ *port-range* } }{**any** | *destination destination-wildcard*} {**any** | *destination-port*/ *port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**disable-port**]

[**sequence** *value*] **deny** *udp* {**any** | *source source-wildcard*} {**any** | *source-port/ port-range*} {**any** | *destination destination-wildcard*} {**any** | *destination-port/ port-range*} [**dscp** *number* | **precedence** *number*] [**disable-port**]

no sequence *value*

Parameters

- **sequence** *value*—(Optional) Specifies the sequence number of the IPv4-based ACL. The acceptable range is from 1 to 2147483547. If not specified, the switch provides a number starting from 1 in ascending order.
- *protocol*—The name or the number of an IP protocol. Available protocol names are icmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, and isis. To match any protocol, use the **ip** keyword. (Range: 0 to 255)
- *source*—Source IP address of the packet.
- *source-wildcard*—Wildcard bits to be applied to the source IP address.
- *source-port/port range*—UDP or TCP source port. Predefined port names are defined in the *destination-port/port-range* parameter. (Range: 0 to 65535)
- *destination*—Destination IP address of the packet.
- *destination-wildcard*—Wildcard bits to be applied to the destination IP address.
- *destination-port/port range*—UDP or TCP destination port. You can enter a range of ports by using hyphen, such as 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (35), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (135), non500-isakmp (4500), ntp (123), rip (520), snmp 161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (35), who (513), or xdmcp (177). (Range: 0 to 65535)
- **dscp** *number*—(Optional) Specifies the DSCP value.
- **precedence** *number*—(Optional) Specifies the IP precedence value.

- **disable-port**—(Optional) The Ethernet interface is disabled if the condition is matched.
- *icmp-type*—(Optional) The ICMP message type for filtering ICMP packets. Enter a number or one of these values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, or photuris. (Range: 0 to 255)
- *icmp-code*—(Optional) ICMP message code for filtering ICMP packets. (Range: 0 to 255)
- **match-all** *list-of-flags*—(Optional) Specifies a list of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. The flags are concatenated to one string, such as +fin-ack.

Default Configuration

No IPv4-based ACE is defined.

Command Mode

IP Access-List Configuration mode

User Guidelines

After an ACE is added to an ACL, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

The number of TCP or UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP.

If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE.

If a range of ports is used for a destination port in ACE, it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for a source port, it is counted again if it is also used for a destination port.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-acl)# deny ip 172.212.0.0/0.0.255.255 any
```

deny (IPv6)

To set deny conditions for an IPv6-based ACL, use the **deny** IPv6 Access-List Configuration mode command.

To remove an IPv6-based ACE, use the **no sequence** command.

Syntax

[**sequence** *value*] **deny** *protocol* {**any** | *source-prefix/length*} {**any** | *destination-prefix/length*} [**dscp** *number*| **precedence** *number*] [**disable-port**]

[**sequence** *value*] **deny** *icmp* {**any** | *source-prefix* {**any** | *source-prefix/length* } {**any** | *destination- prefix/length*} {**any** | *icmp-type*} {**any** | *icmp-code*} [**dscp** *number*| **precedence** *number*] [**disable-port**]

[**sequence** *value*] **deny** *tcp* {**any** | *source-prefix/length*} {**any** | *source-port/port-range*} {**any** | *destination- prefix/length*} {**any**| *destination-port/port-range*} [**dscp** *number*| **precedence** *number*] [**match-all** *list-of-flags*] [**disable-port**]

[**sequence** *value*] **deny** *udp* {**any** | *source-prefix/length*} {**any** | *source-port/port-range*} {**any** | *destination- prefix/length*} {**any** | *destination-port/port-range*} [**dscp** *number*| **precedence** *number*] [**match-all** *list-of-flags*] [**disable-port**]

no sequence *value*

Parameters

- **sequence** *value*—(Optional) Specifies the sequence number of the IPv6-based ACL. The acceptable range is from 1 to 2147483547. If not specified, the switch provides a number starting from 1 in ascending order.
- *protocol*—The name or the number of an IP protocol. Available protocol names are icmp (58), tcp (6), and udp (17). To match any protocol, use the **ipv6** keyword. (Range: 0 to 255)
- *source-prefix/length*—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the format

documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- *source-port/port-range*—The UDP or TCP source port. Predefined port names are defined in the *destination-port/port-range* parameter. (Range: 0 to 65535)
- *destination-prefix/length*—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- *destination-port/port-range*—The UDP or TCP destination port. You can enter a range of ports by using a hyphen, such as 20 - 21. For TCP enter a number or one of these values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data 20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), or xdmcp (177). (Range: 0 to 65535)
- **dscp** *number*—(Optional) Specifies the DSCP value. (Range: 0 to 63)
- **precedence** *number*—(Optional) Specifies the IP precedence value.
- **disable-port**—(Optional) Disables the Ethernet interface if the condition is matched.
- *icmp-type*—(Optional) The ICMP message type for filtering ICMP packets. Enter a number or one of these values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), or nd-na (135). (Range: 0 to 255)
- *icmp-code*—(Optional) The ICMP message code for filtering ICMP packets. (Range: 0 to 255)
- **match-all** *list-of-flags*—(Optional) Specifies a list of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -

urg, -ack, -psh, -rst, -syn, and -fin. The flags are concatenated to one string, such as +fin-ack.

Default Configuration

No IPv6-based ACE is defined.

Command Mode

IPv6 Access-List Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP.

If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE.

If a range of ports is used for a destination port in ACE, it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for a source port, it is counted again if it is also used for a destination port.

Example

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-acl)# deny tcp 3001::2/64 any any 80
```

ip access-group in

To bind an IPv4-based ACL to an interface, use the **ip access-group in** Interface Configuration mode command.

To remove all IPv4-based ACLs from an interface, use the **no** form of this command.

Syntax

ip access-group *acl-name* **in**

no ip access-group in

Parameters

- *acl-name*—Name of the IPv4-based ACL. (Range: 1 to 32 characters)

Default Configuration

No IPv4-based ACL is applied to the interface.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# ip access-group v4acl1 in
```

ip access-list extended

To name an IPv4-based ACL and to enter the IPv4 Access-List Configuration mode, use the **ip access-list extended** Global Configuration mode command.

To remove an IPv4-based ACL, use the **no** form of this command.

Syntax

ip access-list extended *acl-name*

no ip access-list extended *acl-name*

Parameters

- *acl-name*—Name of the IPv4-based ACL. (Range: 1 to 32 characters)

Default Configuration

No IPv4-based ACL is configured.

Command Mode

Global Configuration mode

User Guidelines

The IPv4-based ACEs for this IPv4-based ACL are defined in the **permit (IP)** and **deny (IP)** commands.

An IPv4-based ACL is defined by a unique name. IPv4-based ACL, IPv6-based ACL, MAC-based ACL, or policy map cannot have the same name.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-acl)#
```

ipv6 access-group in

To bind an IPv6-based ACL to an interface, use the **ipv6 access-group in** Interface Configuration mode command.

To remove all IPv6-based ACLs from an interface, use the **no** form of this command.

Syntax

ipv6 access-group *acl-name* **in**

no ipv6 access-group in

Parameters

- *acl-name*—Name of the IPv6-based ACL. (Range: 1 to 32 characters)

Default Configuration

No IPv6-based ACL is applied to the interface.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# ipv6 access-group v6acl1 in
```

ipv6 access-list

To define an IPv6-based ACL and to enter the IPv6 Access-List Configuration mode, use the **ipv6 access-list** Global Configuration mode command.

To remove an IPv6-based ACL, use the **no** form of this command.

Syntax

ipv6 access-list *acl-name*

no ipv6 access-list *acl-name*

Parameters

- *acl-name*—Name of the IPv6-based ACL. (Range: 1 to 32 characters)

Default Configuration

No IPv6-based ACL is defined.

Command Mode

Global Configuration mode

User Guidelines

The IPv6-based ACEs for this IPv6-based ACL are defined in the **permit (IPv6)** and **deny (IPv6)** commands.

An IPv6-based ACL is defined by a unique name. IPv4-based ACL, IPv6-based ACL, MAC-based ACL, or policy map cannot have the same name.

Each IPv6-based ACL has implicit **permit icmp any any nd-ns any, permit icmp any any nd-na any**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process uses the IPv6 network layer service, therefore, by default, IPv6-based ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data link layer protocol; therefore, by default, IPv4-based ACLs implicitly allow ARP packets to be sent and received on an interface.

Example

```
switchxxxxxx(config)# ipv6 access-list test
```

```
switchxxxxxx(config-ipv6-acl)#
```

mac access-group in

To bind a MAC-based ACL to an interface, use the **mac access-group in** Interface Configuration mode command.

To remove all MAC-based ACLs from an interface, use the **no** form of this command.

Syntax

mac access-group *acl-name* **in**

no mac access-group in

Parameters

- *acl-name*—Name of the MAC-based ACL. (Range: 1 to 32 characters)

Default Configuration

No MAC-based ACL is applied to the interface.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
witchxxxxxx(config)# interface gi11
witchxxxxxx(config-if)# mac access-group macac11 in
```

mac access-list extended

To define a Layer 2 ACL based on source MAC address filtering and to enter the MAC Access-List Configuration mode, use the **mac access-list extended** Global Configuration mode command.

To remove a MAC-based ACL, use the **no** form of this command.

Syntax

mac access-list extended *acl-name*

no mac access-list extended *acl-name*

Parameters

- *acl-name*—Name of the MAC-based ACL. (Range: 1 to 32 characters)

Default Configuration

No MAC-based ACL is defined.

Command Mode

Global Configuration mode

User Guidelines

The MAC-based ACEs for this MAC-based ACL are defined in the **permit (MAC)** and **deny (MAC)** commands.

A MAC-based ACL is defined by a unique name. IPv4-based ACL, IPv6-based ACL, MAC-based ACL, or policy map cannot have the same name.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

no sequence

To remove a permit or deny ACE for an IPv4-based ACL, an IPv6-based ACL, or a MAC-based ACL, use the **no sequence** command in the IP Access-List Configuration mode, in the IPv6 Access-List Configuration mode, or in the MAC Access-List Configuration mode.

Syntax

no sequence *value*

Parameters

- *value*—Sequence name of the ACL. The acceptable range is from 1 to 2147483547.

Command Mode

IP Access-List Configuration mode, IPv6 Access-List Configuration mode, and MAC Access-List Configuration mode

Example

```
switchxxxxxx(config)# mac access-list extended macac11
switchxxxxxx(config-mac-acl)# show access-list

MAC access list macac11
....sequence 1 permit any any

switchxxxxxx(config-mac-acl)# no sequence 1
```

permit (IP)

To set permit conditions for an IPv4-based ACL, use the **permit** IP Access-List Configuration mode command.

To remove an IPv4-based ACE, use the **no sequence** command.

Syntax

[**sequence** *value*] **permit** *protocol* {**any** | *source source-wildcard* } {**any** | *destination destination-wildcard* } [**dscp** *number* | **precedence** *number*]

[**sequence** *value*] **permit** *icmp* {**any** | *source source-wildcard* } {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*] [**dscp** *number* | **precedence** *number*]

[**sequence** *value*] **permit** *tcp* {**any** | *source source-wildcard* } {**any** | *source-port/ port-range*} {**any** | *destination destination-wildcard* } {**any** | *destination-port/ port-range* } [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*]

[**sequence** *value*] **permit** *udp* {**any** | *source source-wildcard* } {**any** | *source-port/ port-range* } {**any** | *destination destination-wildcard* } {**any** | *destination-port/ port-range* } [**dscp** *number* | **precedence** *number*]

no sequence *value*

Parameters

- **sequence** *value*—(Optional) Specifies the sequence number for the IPv4-based ACL. The acceptable range is from 1 to 2147483547. If not specified, the switch provides a number starting from 1 in ascending order.
- *protocol*—The name or the number of an IP protocol. Available protocol names are icmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, and isis. To match any protocol, use the **IP** keyword. (Range: 0 to 255)
- *source*—Source IP address of the packet.
- *source-wildcard*—Wildcard bits to be applied to the source IP address.
- *source-port/port-range*—(Optional) The UDP or TCP source port. Predefined port names are defined in the *destination-port/port-range* parameter. (Range: 0 to 65535)
- *destination*—Destination IP address of the packet.
- *destination-wildcard*—Wildcard bits to be applied to the destination IP address.
- *destination-port/port-range*—(Optional) The UDP or TCP destination port. You can enter a range of ports by using hyphen such as 20 - 21. For TCP enter a number or one of these values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (35), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (135), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (35), who (513), or xdmcp (177). (Range: 0 to 65535)
- **dscp** *number*—(Optional) Specifies the DSCP value.
- **precedence** *number*—(Optional) Specifies the IP precedence value.
- *icmp-type*—(Optional) The ICMP message type for filtering ICMP packets. Enter a number or one of these values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply,

address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, or photuris. (Range: 0 to 255)

- *icmp-code*—(Optional) The ICMP message code for filtering ICMP packets. (Range: 0 to 255)
- **match-all** *list-of-flags*—(Optional) Specifies a list of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. The flags are concatenated to one string, such as +fin-ack.

Default Configuration

No IPv4-based ACE is defined.

Command Mode

IP Access-List Configuration mode

User Guidelines

After an ACE is added to an ACL, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP.

If a range of ports is used for a source port in an ACE, it is not counted again if it is also used for a source port in another ACE.

If a range of ports is used for a destination port in an ACE, it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for a source port, it is counted again if it is also used for a destination port.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-acl)# permit ip 176.212.0.0 0.0.255.255 any
```

permit (IPv6)

To set permit conditions for an IPv6-based ACL, use the **permit** command in the IPv6 Access-List Configuration mode.

To remove an IPv6-based ACE, use the **no sequence** command.

Syntax

[**sequence** *value*] **permit** *protocol* {**any** | *source-prefix/length* } {**any** | *destination-prefix/length* } [**dscp** *number* | **precedence** *number*]

[**sequence** *value*] **permit** *icmp* {**any** | {*source-prefix/length* } {**any** | *destination-prefix/length* } {**any** | *icmp-type* } {**any** | *icmp-code* } [**dscp** *number* | **precedence** *number*]

[**sequence** *value*] **permit** *tcp* {**any** | *source-prefix/length* } {**any** | *source-port/port-range*} {**any** | *destination- prefix/length*} {**any** | *destination-port| port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*]

[**sequence** *value*] **permit** *udp* {**any** | *source-prefix/length* } {**any** | *source-port/port-range*} {**any** | *destination- prefix/length*} {**any** | *destination-port/port-range*} [**dscp** *number* /**precedence** *number*]

no sequence *value*

Parameters

- **sequence** *value*—(Optional) The sequence number for the IPv6-based ACL. The acceptable range is from 1 to 2147483547. If not specified, the switch provides a number starting from 1 in ascending order.
- *protocol*—The name or the number of an IP protocol. Available protocol names are icmp (58), tcp (6), and udp (17). To match any protocol, use the **ipv6** keyword. (Range: 0 to 255)
- *source-prefix/length*—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- *source-port/port-range*—The UDP or TCP source port. Predefined port names are defined in the *destination-port/port-range* parameter. (Range: 0 to 65535)
- *destination-prefix/length*—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in

the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- *destination-port/port-range*—The UDP or TCP destination port. You can enter a range of ports by using a hyphen, such as 20 - 21. For TCP enter a number or one of these values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (35), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (135), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (35), who (513), or xdmcp (177). (Range: 0 to 65535)
- **dscp** *number*—(Optional) Specifies the DSCP value. (Range: 0 to 63)
- **precedence** *number*—(Optional) Specifies the IP precedence value.
- *icmp-type*—(Optional) The ICMP message type for filtering ICMP packets. Enter a number or one of these values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), or nd-na (135). (Range: 0 to 255)
- *icmp-code*—(Optional) The ICMP message code for filtering ICMP packets. (Range: 0 to 255)
- **match-all** *list-of-flag*—(Optional) Specifies a list of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. The flags are concatenated to one string, such as +fin-ack.

Default Configuration

No IPv6-based ACE is defined.

Command Mode

Ipv6 Access-List Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP.

If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE.

If a range of ports is used for a destination port in ACE, it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for a source port, it is counted again if it is also used for a destination port.

Example

This example defines an IPv6-based ACL by the server name and enters an IPv6-based ACE for TCP packets:

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-acl)# permit tcp 3001::2/64 any any 80
```

permit (MAC)

To set permit conditions for a MAC-based ACL, use the **permit** command in the MAC Access-List Configuration mode.

To remove a MAC-based ACE, use the **no sequence** command.

Syntax

[**sequence** *value*] **permit** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | **vlan** *vlan-id*] [**cos** *cos cos-wildcard*] [**ethtype** *value*]

no sequence *value*

Parameters

- **sequence** *value*—(Optional) Specifies the sequence number for the MAC-based ACL. The acceptable range is from 1 to 2147483547. If not specified, the switch provides a number starting from 1 in ascending order.
- *source*—Source MAC address of the packet.

- *source-wildcard*—Wildcard bits to be applied to the source MAC address.
- *destination*—Destination MAC address of the packet.
- *destination-wildcard*—Wildcard bits to be applied to the destination MAC address.
- **vlan** *vlan-id*—(Optional) Specifies the VLAN ID of the packet. (Range: 1 to 4094)
- *cos*—(Optional) The CoS value of the packet. (Range: 0 to 7)
- *cos-wildcard*—(Optional) Wildcard bits to be applied to the CoS.
- **ethtype** *value*—(Optional) Specifies the Ethernet type in hexadecimal format of the packet. (Range: 1501 to 65535)

Default Configuration

No MAC-based ACE is defined.

Command Mode

MAC Access-List Configuration mode

User Guidelines

After an ACE is added to an ACL, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

show access-lists

To display the ACLs for a specific class defined on the switch, use the **show access-lists** Privileged EXEC mode command.

Syntax

show {**ip** | **ipv6** | **mac**} **access-lists** [*acl-name*]

Parameters

- **ip | ipv6 | mac**—Specifies the ACL type.
- *acl-name*—(Optional) Name of the ACL. (Range: 1 to 32 characters)

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip access-lists
```

show access-lists

To display all ACLs configured on the switch, use the **show access-lists** Privileged EXEC mode command.

Syntax

show access-lists

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show access-lists

MAC access list macacl1
    sequence 1 permit any any cos 7 5

IPv6 access list v6acl1
    sequence 1 permit ipv6 abcd::/64 aacc::/64
```

show access-lists utilization

To display the utilization of the access-list group, use the **show access-lists utilization** Privileged EXEC mode command.

Syntax

show access-lists utilization

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show access-lists utilization
Max TCAM entries: 1408
In used: 0
```

5

Address Table Commands

bridge multicast reserved-address

To define the action on multicast reserved-address packets, use the **bridge multicast reserved-address** Global Configuration mode command.

Syntax

bridge multicast reserved-address *mac-multicast-address* {**discard** | **bridge** | **peer**}

Parameters

- *mac-multicast-address*—Multicast MAC address to be reserved.
- **bridge**—Forwards the packets.
- **discard**—Discards the packets.
- **peer**—Processes the packets based on its protocols or applications.

Default Configuration

If the MAC address is not used by any protocol, the default action is bridge.

Command Mode

Global Configuration mode

User Guidelines

The configurations (that contain service type) have precedence over less specific configurations (that contain only MAC address).

The packets that are bridged are subject to security ACLs.

The action defined by this command has precedence over the forwarding rules defined by the applications or protocols (such as STP and LLDP) supported on the switch.

Example

```
switchxxxxxx(config)# bridge multicast reserved-address 00:3f:bd:45:5a:b1
discard
```

clear mac address-table

To clear the learned entries from the forwarding database (FDB), use the **clear mac address-table** Privileged EXEC command.

Syntax

clear mac address-table dynamic [**interfaces** *interface-id* | **vlan** *vlan-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Deletes all dynamic (learned) addresses on specific interfaces. The interface can be one of these types: Ethernet port, or port channel.
- **vlan** *vlan-id*—(Optional) Deletes all secure addresses learned on a VLAN.

Default Configuration

If no interface or VLAN is specified, all entries in the dynamic MAC address table will be cleared.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear mac address-table dynamic interfaces gi11
```

mac address-table aging-time

To set the aging time of the MAC address table, use the **mac address-table aging-time** Global Configuration mode command.

Syntax

mac address-table aging-time *seconds*

Parameters

- *seconds*—The time in seconds that an entry remains in the MAC address table. (Range:10 to 1000000 seconds, 0 indicates no aging)

Default Configuration

The default aging time is 300 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# mac address-table aging-time 600
```

mac address-table static

To add a MAC-layer station source address to the MAC address table, use the **mac address-table static** Global Configuration mode command.

To delete a MAC address from the MAC address table, use the **no** form of this command.

Syntax

mac address-table static *mac-address* **vlan** *vlan-id* **interfaces** *interface-id* [**delete-on-reboot** | **delete-on-timeout** | **permanent** | **secure**]

mac address-table static *mac-address* **vlan** *vlan-id* **drop**

no mac address-table static *mac-address* **vlan** *vlan-id*

Parameters

- *mac-address*—MAC address of the interface.
- **vlan** *vlan-id*—VLAN ID for the interface.
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.
- **delete-on-reboot**—(Optional) Specifies that the static MAC address is never aged out of the table and will be deleted after the switch reboots.
- **delete-on-timeout**—(Optional) Deletes the MAC address when aging occurs.
- **permanent**—(Optional) Specifies that the static MAC address never be aged out of the table and if it is saved to the Startup Configuration, it is retained after rebooting. The keyword is applied by the default.
- **secure**—(Optional) Specifies that the MAC address is secure when the interface is in classic locked mode.
- **drop**—Drops the packets with the specified source or destination unicast MAC address.

Default Configuration

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

Command Mode

Global Configuration mode

User Guidelines

Use the command to add a static MAC address with the given time-to-live in any mode or to add a secure MAC address in a secure mode.

Each MAC address in the MAC address table is assigned two attributes: **type** and **time-to-live**.

The following time-to-live values are supported:

- **delete-on-reboot**—A MAC address is saved until the next reboot.
- **delete-on-timeout**—A MAC address that may be removed by the aging timer.
- **permanent**—A MAC address is saved until it is removed manually.

The following types are supported:

- **static**— MAC address is manually added by the command with the following keywords specifying its time-to-live:
  - **permanent**
  - **delete-on-reboot**
  - **delete-on-timeout**

  A static MAC address may be added in any port mode.
- **secure**—A MAC address added manually or learned in a secure mode. Use the **mac address-table static** command with the secure keyword to add a secure MAC address. The MAC address cannot be relearned. A secure MAC address may be added only in a secure port mode.
- **dynamic**—A MAC address learned by the switch in nonsecure mode. A value of its time-to-live attribute is **delete-on-timeout**.

Examples

Example 1—The following example adds two permanent static MAC addresses:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1
interfaces gi1
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interfaces gi1 permanent
```

Example 2—The following example adds a deleted-on-reboot static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interfaces gi1 delete-on-reboot
```

Example 3—The following example adds a deleted-on-timeout static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interfaces gi1 delete-on-timeout
```

Example 4—The following example adds a secure MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interfaces gi1 secure
```

show bridge multicast reserved-address

To show information for all reserved MAC addresses, use the **show bridge multicast reserved-address** Privileged EXEC mode command.

Syntax

show bridge multicast reserved-address

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx # show bridge multicast reserved-address
Reserved mac-address | action
---------------------+---------
  01:80:C2:00:00:02   |  peer
  01:80:C2:00:00:03   |  bridge
  01:80:C2:00:00:04   |  bridge
  01:80:C2:00:00:05   |  bridge
  01:80:C2:00:00:06   |  bridge
  01:80:C2:00:00:07   |  bridge
  01:80:C2:00:00:08   |  bridge
  01:80:C2:00:00:09   |  bridge
  01:80:C2:00:00:0A   |  bridge
  01:80:C2:00:00:0B   |  bridge
  01:80:C2:00:00:0C   |  bridge
  01:80:C2:00:00:0D   |  bridge
  01:80:C2:00:00:0E   |  bridge
  01:80:C2:00:00:0F   |  bridge
  01:80:C2:00:00:10   |  bridge
  01:80:C2:00:00:11   |  bridge
  01:80:C2:00:00:12   |  bridge
  01:80:C2:00:00:13   |  bridge
  01:80:C2:00:00:14   |  bridge
  01:80:C2:00:00:15   |  bridge
  01:80:C2:00:00:16   |  bridge
  01:80:C2:00:00:17   |  bridge
  01:80:C2:00:00:18   |  bridge
```

```
01:80:C2:00:00:19   |  bridge
01:80:C2:00:00:1A   |  bridge
01:80:C2:00:00:1B   |  bridge
01:80:C2:00:00:1C   |  bridge
01:80:C2:00:00:1D   |  bridge
01:80:C2:00:00:1E   |  bridge
01:80:C2:00:00:1F   |  bridge
01:80:C2:00:00:20   |  bridge
01:80:C2:00:00:21   |  bridge
01:80:C2:00:00:22   |  bridge
01:80:C2:00:00:23   |  bridge
01:80:C2:00:00:24   |  bridge
01:80:C2:00:00:25   |  bridge
01:80:C2:00:00:26   |  bridge
01:80:C2:00:00:27   |  bridge
01:80:C2:00:00:28   |  bridge
01:80:C2:00:00:29   |  bridge
01:80:C2:00:00:2A   |  bridge
01:80:C2:00:00:2B   |  bridge
01:80:C2:00:00:2C   |  bridge
01:80:C2:00:00:2D   |  bridge
01:80:C2:00:00:2E   |  bridge
```

show mac address-table

To show the entries in the MAC address table, use the **show mac address-table** Privileged EXEC command.

Syntax

show mac address-table [**dynamic** | **static**] [**interfaces** *interface-id*] [**vlan** *vlan*]

show mac address-table [*mac-address*] [**vlan** *vlan*]

Parameters

- **dynamic**—(Optional) Displays only dynamic MAC addresses.
- **static**—(Optional) Displays only static MAC addresses.
- **interfaces** *interface-id*—(Optional) Displays the entries for a specific interface. The interface can be one of these types: Ethernet port or port channel.
- **vlan** *vlan*—(Optional) Displays the entries for a specific VLAN.
- *mac-address*—(Optional) Entries for a specific MAC address.

Default Configuration

If no parameters are entered, the entire table is displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Internal usage VLANs that are automatically allocated on the routed ports are presented in the VLAN column by a port number and not by a VLAN ID.

Example

Example 1—Displays the entire MAC address table:

```
switchxxxxxx# show mac address-table
VID    |     MAC Address     |       Type       |    Ports
-----+-------------------+--------------+----------------
    1 | 00:03:6D:00:01:20 |   Management    | CPU
    1 | 00:10:60:DB:6E:FE |     Dynamic     | fa1
    1 | 10:8C:CF:CD:0C:05 |     Dynamic     | fa1

Total number of entries: 3
```

Example 2—Displays the address entries containing the specified MAC address:

```
switchxxxxxx# show mac address-table 00:3f:bd:45:5a:b1 vlan 1
Aging time is 300 sec
VLAN       MAC Address           Port           Type
-------- -----------------   ------------ ----------
1          00:3f:bd:45:5a:b1    static         fa9
```

show mac address-table aging-time

To show the MAC address aging time, use the **show mac address-table aging-time** Privileged EXEC mode command.

Syntax

show mac address-table aging-time

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx # show mac address-table aging-time
Mac Address Table aging time:  300
```

show port-security

To show the port security status, use the **show port-security** Privileged EXEC mode command.

Syntax

show port-security interfaces *interface-id*

Parameters

- **interfaces** *interface-id*—Specifies an Ethernet interface ID or a list of Ethernet interface IDs.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show port-security interfaces fa1-10
  Port    |   Mode   |     Security     | CurrentAddr |        Action        |
Trap Freq
```

```
---------+---------+--------------+------------+-------------------+------
-----
     fa1  | Classic |     Disabled     |       3    |              Discard|
---
     fa2  | Classic |     Disabled     |       0    |              Discard|
---
     fa3  | Classic |     Disabled     |       0    |              Discard|
---
     fa4  | Classic |     Disabled     |       0    |              Discard|
---
     fa5  | Classic |     Disabled     |       0    |              Discard|
---
     fa6  | Classic |     Disabled     |       0    |              Discard|
---
     fa7  | Classic |     Disabled     |       0    |              Discard|
---
     fa8  | Classic |     Disabled     |       0    |              Discard|
---
     fa9  | Classic |     Disabled     |       0    |              Discard|
---
    fa10  | Classic |     Disabled     |       0    |              Discard|
---
```

The following table describes the significant fields shown in the example:

Field	Description
Port	The port number.
Mode	The learning mode: classic or dynamic.
Security	The port security status. The possible values are Enabled or Disabled.
Action	The action taken on violation.
CurrentAddr	The number of addresses currently learned.
Trap Freq	The minimum time interval between consecutive traps.

switchport port-security

To enable the port security on an interface, use the **switchport port-security** Interface Configuration mode command.

To disable the port security on an interface, use the **no** form of this command.

Syntax

switchport port-security

no switchport port-security

Parameters

N/A

Default Configuration

The port security is disabled by default.

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport port-security
```

switchport port-security mode maximum

To set the port security learning mode and the maximum number of MAC addresses that can be learned on an interface, use the **switchport port-security mode maximum** Interface Configuration mode command.

To revert to its default settings, use the **no** form of this command.

Syntax

switchport port-security mode {**classic** | **dynamic**} **maximum** *max-addr* **action** { **discard** | {**discard-snmp-log trap-freq** *seconds*} | {**discard-snmp-log-shutdown trap-freq** *seconds*} | **forward**}

no switchport port-security maximum

Parameter

- **classic**— Classic lock. All learned MAC addresses on the port are locked and the switch learns up to the maximum number of addresses allowed on the port. The learned addresses are not subject to aging or re-learning.

- **dynamic**— Limited dynamic lock. The switch learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the switch does not learn additional addresses. In this mode, the addresses are subject to aging and relearning.
- *max-addr*—Maximum number of MAC addresses that can be learned on the port.
- **action**— The action to be applied to the packets arriving on a locked port.
  - **discard**—Discards the packets with unlearned source addresses.
  - **discard-snmp-log**—Discards the packets with unlearned source addresses, an SNMP trap is sent, and a SYSLOG message is logged.
  - **discard-snmp-log-shutdown**—Discards the packets with unlearned source addresses, an SNMP trap is sent, a SYSLOG message is logged, and shuts down the port.
  - **forward**—Forwards the packets with unlearned source addresses, but does not learn the address.
- **trap-freq** *seconds*—Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1 to 1000000)

Default Configuration

The feature is disabled by default.

The default mode is **discard**.

The default number of seconds is zero, but if **discard-snmp-log** or **discard-snmp-log-shutdown** is entered, **trap-freq** *seconds* must also be entered.

Command Mode

Interface Configuration mode

User Guidelines

The command may be used only when the interface is in the regular mode (nonsecure with unlimited MAC learning).

See the **mac address-table static** command for information about MAC address attributes (type and time-to-live).

When the **switchport port-security** command enables the **lock** mode on a port, all dynamic addresses learned on the port are changed to permanent secure addresses.

When the **switchport port-security** command enables a mode on a port differing from the **lock** mode, all addresses learned on the port are deleted.

When the **no switchport port-security maximum** command cancels a secure mode on a port, all secure addresses defined on the port are deleted.

Example

The following example discards all packets to gi11 when the learning reaches the address limit (50) without learning any more addresses of packets from unknown sources, and sends the SNMP traps every 100 seconds if a packet with an unknown source address is received.

```
switchxxxxxx(config)interface gi11
switchxxxxxx(config-if)# switchport port-security mode classic maximum 50
action discard-snmp-log trap-freq 100
```

6

Bonjour Commands

bonjour enable

To enable Bonjour globally on the switch, use the **bonjour enable** Global Configuration mode command.

To disable Bonjour, use the **no** form of this command.

Syntax

bonjour enable

no bonjour enable

Parameters

N/A

Default Configuration

Bonjour is enabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# bonjour enable
```

show bonjour

To show Bonjour information, use the **show bonjour** Privileged EXEC Configuration mode command.

Syntax

show bonjour

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the Bonjour service information:

```
switchxxxxxx# show bonjour
Bonjour status: enabled
L2 interface status: Up
IP Address: 192.168.1.254

Service     Admin Status    Oper Status
--------    ------------    -----------
csco-sb     enabled         enabled
csco-api    enabled         enabled
https       enabled         enabled
http        enabled         enabled
ssh         enabled         disabled
telnet      enabled         disabled
```

7

CDP Commands

cdp advertise-v2

To use Cisco Discovery Protocol (CDP) version 2 for all transmitted CDP packets, use the **cdp advertise-v2** Global Configuration mode command.

To use CDP version 1, use the **no** form of this command.

Syntax

cdp advertise-v2

no cdp advertise-v2

Parameters

N/A

Default Configuration

CDP version 2 is used by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# cdp advertise-v2
```

cdp appliance-vlan enable

To enable the switch to advertise the voice VLAN in CDP packets on all interfaces that are CPD-enabled and are members of the voice VLAN, use the **cdp appliance-vlan enable** Global Configuration mode command.

To disable CDP voice VLAN advertisement, use the **no** form of this command.

Syntax

cdp appliance-vlan enable

no cdp appliance-vlan enable

Parameters

N/A

Default Configuration

CDP voice VLAN advertisement is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This MIB specifies the voice VLAN ID (VVID) to which this interface belongs:

- **0**—CDP packets transmitting through this interface will contain Appliance VLAN-ID TLV with the value of 0. VoIP and related packets are expected to be sent and received with the value of 0 (VLAN ID=0) and a 802.1p priority.
- **1 to 4094**—CDP packets transmitting through this interface will contain Appliance VLAN-ID TLV with N. VoIP and related packets are expected to be sent and received with the value of N (VLAN ID=N) and a 802.1p priority.
- **4095**—CDP packets transmitting through this interface will contain Appliance VLAN-ID TLV with the value of 4095. VoIP and related packets are expected to be sent and received untagged without a 802.1p priority.
- **4096**—CDP packets transmitting through this interface will not include Appliance VLAN-ID TLV. If the VVID is not supported on the interface, this MIB object will not be configurable and will return 4096.

Example

```
switchxxxxxx(config)# cdp appliance-vlan enable
```

cdp device-id format

To specify the format of Device-ID TLV, use the **cdp device-id format** Global Configuration mode command.

Syntax

cdp device-id format {**mac** | **serial-number** | **hostname**}

Parameters

- **mac**—The Device-ID TLV contains the MAC address of the switch.
- **serial-number**—The Device-ID TLV contains the hardware serial number of the switch.
- **hostname**—The Device-ID TLV contains the hostname of the switch.

Default Configuration

The MAC address of the switch is contained by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp device-id format serial-number
```

cdp enable

To enable CDP on an interface, use the **cdp enable** Interface Configuration mode command.

To disable CDP on an interface, use the **no** form of this command.

Syntax

cdp enable

no cdp enable

Parameters

N/A

Default Configuration

CDP is enabled on each interface by default.

Command Mode

Interface Configuration mode

User Guidelines

To enable CDP on an interface, you must first enable CDP globally on the switch by using the **cdp run** command.

Example

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# interface fa5
switchxxxxxx(config-if)# cdp enable
```

cdp holdtime

To specify the number of seconds that CDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval, use the **cdp holdtime** Global Configuration mode command.

Syntax

cdp holdtime *seconds*

Parameters

- *seconds*—Number of seconds that a receiver must keep the advertised CDP information. The holdtime should be bigger than the value of the transmission timer. (Range: 10 to 255 seconds)

For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the CDP packets are discarded after 120 seconds.

Default Configuration

The default CDP holdtime is 180 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp holdtime 120
```

cdp log mismatch duplex

To enable validating that the duplex status of an interface received in a CDP packet matches its actual configuration, use the **cdp log mismatch duplex** Interface Configuration mode command.

To disable generating the SYSLOG messages for duplex mismatches, use the **no** form of this command.

Syntax

cdp log mismatch duplex

no cdp log mismatch duplex

Parameters

N/A

Default Configuration

The switch reports the duplex mismatches from all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

When duplex information is mismatched, which means that the duplex information in the incoming frame does not match what the local device is advertising, a SYSLOG duplex mismatch message is generated by CDP.

Example

```
switchxxxxxx(config)# interface fa11
switchxxxxxx(config-if)# cdp log mismatch duplex
```

cdp log mismatch native

To enable validating that the native VLAN received in a CDP packet matches the actual native VLAN of the interface, use the **cdp log mismatch native** Interface Configuration mode command.

To disable generating the SYSLOG messages for native VLAN mismatches, use the **no** form of this command.

Syntax

cdp log mismatch native

no cdp log mismatch native

Parameters

N/A

Default Configuration

The switch reports the native VLAN mismatches from all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

When a native VLAN mismatch is detected, which means that the native VLAN information in the incoming frame does not match what the local device is advertising, a SYSLOG message is generated by CDP.

Example

```
switchxxxxxx(config)# interface fa11
switchxxxxxx(config-if)# cdp log mismatch native
```

cdp log mismatch voip

To enable validating that the VoIP status of the interface received in a CDP packet matches its actual configuration, use the **cdp log mismatch voip** Interface Configuration mode command.

To disable generating the SYSLOG messages for VoIP mismatches, use the **no** form of this command.

Syntax

cdp log mismatch voip

no cdp log mismatch voip

Parameters

N/A

Default Configuration

The switch reports the VoIP mismatches from all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

When a voice VLAN mismatch is detected, which means that the voice VLAN information in the incoming frame does not match what the local device is advertising, a SYSLOG message is generated by CDP.

Example

```
switchxxxxxx(config)# interface fa11
switchxxxxxx(config-if)# cdp log mismatch voip
```

cdp mandatory-tlvs validation

To validate that all mandatory (according to CDP protocol) TLVs are present in the received CDP frames, use the **cdp mandatory-tlvs validation** Global Configuration mode command.

To disable the CDP mandatory TLVs validation, use the **no** form of this command.

Syntax

cdp mandatory-tlvs validation

no cdp mandatory-tlvs validation

Parameters

N/A

Default Configuration

CDP mandatory TLVs validation is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

If the CDP mandatory TLVs validation is enabled, incoming CDP packets not containing the mandatory TLVs are discarded and the invalid error counter is incremented.

Example

```
switchxxxxxx(config)# cdp mandatory-tlvs validation
```

cdp pdu

To specify how to deal with CDP packets when CDP is disabled globally, use the **cdp pdu** Global Configuration mode command.

Syntax

cdp pdu {**bridging** | **filtering** | **flooding**}

Parameters

- **bridging**—When CDP is globally disabled, bridges CDP packets as regular data packets (forwarded based on VLAN).
- **filtering**—When CDP is globally disabled, filters (deletes) CDP packets.
- **flooding**—When CDP is globally disabled, floods CDP packets to all ports that are in the STP forwarding state, ignoring the VLAN filtering rules.

Default Configuration

Bridging

Command Mode

Global Configuration mode

User Guidelines

When CDP is globally enabled, CDP packets are filtered (discarded) on the CDP-disabled ports.

In the flooding mode, the VLAN filtering rules are not applied, but the STP rules are applied. In case of MSTP, CDP packets are classified to the instance 0.

Example

The following example specifies that when CDP is globally disabled, CDP packets are flooded to all ports that are in the STP forwarding state:

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# cdp pdu flooding
```

cdp run

To enable CDP globally on the switch, use the **cdp run** Global Configuration mode command.

To disable CDP globally on the switch, use the **no** form of this command.

Syntax

cdp run

no cdp run

Parameters

N/A

Default Configuration

CDP is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

CDP is a link-layer protocol for directly connected CDP devices to advertise themselves and their capabilities. In deployments where the CDP-capable devices are not directly connected and are separated with the CDP-incapable devices, the CDP-capable devices may be able to receive the advertisement from other device(s) only if the CDP-incapable devices flood the CDP packets that they receive. If the CDP-incapable devices perform VLAN-aware flooding, then the CDP-capable devices can hear each other only if they are in the same VLAN. It should be noted that a CDP-capable device may receive the advertisement from more than one device if the CDP-incapable devices flood the CDP packets.

To learn and advertise CDP information, CDP must be globally enabled and also enabled on the interfaces. By default, CDP is enabled globally and enabled on all interfaces.

Example

```
switchxxxxxx(config)# cdp run
```

cdp timer

To specify how often CDP packets are transmitted, use the **cdp timer** Global Configuration mode command.

Syntax

cdp timer *seconds*

Parameters

- *seconds*—Enter the rate in seconds at which CDP advertisement updates are sent. (Range: 5 to 254 seconds)

Default Configuration

The default transmission timer is 60 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp timer 200
```

clear cdp counter

To reset the CDP traffic counters to 0, use the **clear cdp counter** Privileged EXEC Mode command.

Syntax

clear cdp counter

Parameters

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# clear cdp counter
```

clear cdp table

To delete all entries in the CDP cache table, use the **clear cdp table** Privileged EXEC Mode command.

Syntax

clear cdp table

Parameters

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# clear cdp table
```

show cdp

To show the CDP global settings, use the **show cdp** Privileged EXEC mode command.

Syntax

show cdp

Parameters

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show cdp
CDP Global Configuration:
         CDP is globally enabled
```

```
CDP log duplex mismatch is globally enabled
CDP log native VLAN mismatch is globally enabled
CDP log voice VLAN mismatch is globally enabled
Mandatory TLVs validation is enabled
Sending CDPv2 advertisements is enabled
Sending Appliance TLV is enabled
Device ID format is Host name
Sending CDP packets every 200 seconds
Sending a holdtime value of 180 seconds
CDP packets handling mode is flooding
```

show cdp entry

To show information for all CDP neighbors or for a specific CDP neighbor, use the **show cdp entry** Privileged EXEC mode command. You can limit the display to protocol or version information.

Syntax

show cdp entry {***** | **WORD**} [**protocol** | **version**]

Parameters

- ***—**Displays information for all CDP neighbors.
- **WORD—**Displays information for a specific CDP neighbor. You need to specify the name of the CDP neighbor (its device ID) to be displayed.
- **protocol—**(Optional) Displays information about the protocols enabled on the CDP neighbors.
- **version—**(Optional) Displays information about the software version running on the CDP neighbors.

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show cdp entry * protocol
```

show cdp interfaces

To show information for the interfaces on which CDP is enabled, use the **show cdp interfaces** Privileged EXEC mode command.

Syntax

show cdp interfaces *interface-id*

Parameters

- *interface-id*—The interface ID or a list of interface IDs.

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show cdp interfaces fa11
-------------------------------------------
CDP is globally enabled
CDP log duplex mismatch
  Globally is enabled
  Per interface is enabled
CDP log voice VLAN mismatch
  Globally is enabled
  Per interface is enabled
CDP log native VLAN mismatch
  Globally is enabled
  Per interface is enabled
fa11 is  Down, CDP is enabled
Sending CDP packets every 200 seconds
Holdtime is 180 seconds
```

show cdp neighbors

The **show cdp neighbors** Privileged EXEC mode command displays information about neighbors

Syntax

show cdp neighbors [**interface-id**] [**detail**]

Parameters

- **interface-id**—Displays the neighbors attached to this port.
- **detail**—Displays detailed information about a neighbor (or neighbors) from the main cache including network address, enabled protocols, hold time, and software version.

Default Configuration

If an interface ID is not specified, the command displays information for the neighbors of all ports.

Command Mode

Privileged EXEC Mode

User Guidelines

The main cache contains the full received CDP messages about limited number of the neighbors.

Use the **show cdp neighbors** [**interface-id**] **detail** command to display the main cache.

Example

```
switchxxxxxx# show cdp neighbor interface fa24
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - VoIP Phone
            Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
          S - Switch, H - Host, I - IGMP, r - Repeater, P - VoIP Phone
          M - Remotely-Managed Device, C - CAST Phone Port,
         W - Two-Port MAC Relay
Device ID       Local      Adv  Holdtime Capability   Platform     Port ID
  Interface  Ver.
------------------ ----------- ---- -------- ---------- ------------ --------
---
Switch150101       fa24       2    178      S I       Cisco SG220- gi48
                                                                        50P
(PID:SG2
                                                    20-50P-K9-NA
                                                                          )
```

show cdp tlv

To show the local device information advertised by the CDP protocol for specific interfaces, use the **show cdp tlv** Privileged EXEC mode command.

Syntax

show cdp tlv *interface-id*

Parameters

- *interface-id*—The interface ID or a list of interface IDs.

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show cdp tlv fa5
CDP is globally enabled

Interface TLV: fa5
CDP is enabled on fa5
Interface fa5 is Up
Device-ID TLV: type is Host name;Value is switchxxxxxx
Address TLV: IPv4 192.168.1.254, IPv6 fe80::66d8:14ff:fe5d:6d36
Port-ID TLV: fa5
Capabilities: Switch IGMP
Version TLV: 1.1.0.9
Platform TLV: MS200X-24P
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN-ID TLV: Appliance-ID is 1; VLAN-ID is 1
Extended Trust TLV: extended trust
COS for Untrusted Ports TLV: 0
```

show cdp traffic global

To show global CDP traffic statistics, use the **show cdp traffic global** Privileged EXEC mode command.

Syntax

show cdp traffic global

Parameters

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show cdp traffic global
CDP counters :
         Total packets output: 101, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 101, Input: 0
```

The following table describes the significant fields shown in the example:

Field	Description
Total packets output, input	Total number of CDP packets received and transmitted on all interfaces.
Hdr syntax	Number of times that packet information could not be stored in cache because of lack of room.
Chksum error	Number of packets received with illegal checksum value.
Invalid packet	Number of packets received with errors other than illegal checksums.
CDP version 1 advertisements output, input	Number of CDP version 1 packets received and transmitted on all interfaces.
CDP version 2 advertisements output, input	Number of CDP version 2 packets received and transmitted on all interfaces.

show cdp traffic (Interface)

To show the CDP traffic counters per interface, use the **show cdp traffic** Privileged EXEC mode command.

Syntax

show cdp traffic [*interface-id*]

Parameters

- *interface-id*—(Optional) The interface ID or a list of interface IDs. If the ID is not specified, this command will display the CDP counters for all interfaces.

Command Mode

Privileged EXEC Mode

User Guidelines

CDP statistics for an interface are only displayed if CDP is enabled globally and on the interface.

Example

```
switchxxxxxx# show cdp traffic
fa1 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
fa2 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
fa3 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
fa4 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
```

```
fa5 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa6 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa7 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa8 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa9 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa10 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa11 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa12 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa13 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
```

```
fa14 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa15 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa16 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa17 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa18 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa19 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa20 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa21 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
fa22 :
        Total packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
        No memory in main cache: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 0, Input: 0
```

```
fa23 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
fa24 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
gi1 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
gi2 :
         Total packets output: 0, Input: 0
         Hdr syntax: 0, Chksum error: 0, Invalid packet: 0
         No memory in main cache: 0
         CDP version 1 advertisements output: 0, Input: 0
         CDP version 2 advertisements output: 0, Input: 0
```

8

Clock Commands

absolute

Use the **absolute** Time-range Configuration mode command to specify an absolute time when a time range is in effect.

Use the **no** form of this command to remove the time limitation.

Syntax

absolute (**end** | **start**) *HH:MM* (**jan** | **feb** | **mar** | **apr** | **may** | **jun** | **jul** | **aug** | **sep** | **oct** | **nov** | **dec**) *<1-31> <2000-2037>*

Parameters

- **start**—Absolute time and date that the permit or deny statement of the associated function going into effect. If no start time and date are specified, the function is in effect immediately.
- **end**—Absolute time and date that the permit or deny statement of the associated function is no longer in effect. If no end time and date are specified, the function is in effect indefinitely.
- **hh:mm**—Time in hours and minutes
- **day**—Day in the month.
- **month**—Month
- **year**—Year

Default Configuration

No default is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the **absolute** command to set the absolute time of time range.

Use the **no** form of this command to remove start or end time.

You can verify your setting by entering the **show time-range Privileged EXEC** command.

Example

The following example shows how to set absolute time:

```
switchxxxxxx(config)#loopback-detection enable
switchxxxxxx (config)# time-range test
switchxxxxxx (config-time-range)# absolute start 09:00 feb 01 2015
switchxxxxxx (config-time-range)# absolute end 18:00 oct 31 2015
switchxxxxxx (config-time-range)# do show time-range test
time-range entry: test (active)
absolute start 09:00 feb 1 2015
absolute end 18:00 oct 31 2015

switchxxxxxx (config-time-range)# no absolute start
switchxxxxxx (config-time-range)# do show time-range test
time-range entry: test (active)
absolute end 18:00 oct 31 2015
```

clock set

To manually set the system clock, use the **clock set** Privileged EXEC mode command.

Syntax

clock set *HH:MM:SS month day year*

Parameters

- *HH:MM:SS*—The current time in hours (military format), minutes, and seconds. (Range: HH: 0 to 23, MM: 0 to 59, SS: 0 to 59)
- *month*—The current month using the first three letters of the month name. (Range: jan–dec)
- *day*—The current day of the month. (Range: 1 to 31)

- *year*—The current year. (Range: 2000 to 2037)

Command Mode

Privileged EXEC mode

Example

The following example sets the system time to 13:32:00 on August 7, 2014:

```
switchxxxxxx# clock set 13:32:00 aug 7 2014
13:32:00 DFL(UTC+8) Aug 07 2014
```

clock source

To configure an external time source for the system clock, use the **clock source** Global Configuration mode command.

Syntax

clock source {**sntp** | **local**}

Parameters

- **sntp**—Specifies an SNTP server as the external clock source.
- **local**—Specifies the local time settings.

Default Configuration

The default is to use the local time as the source of the system clock.

Command Mode

Global Configuration mode

Example

The following example configures the SNTP server as an external time source:

```
switchxxxxxx(config)# clock source sntp
```

clock summer-time

To enable the switch to automatically switch to the summer time (Daylight Saving Time), use the **clock summer-time** Global Configuration mode command.

To disable this feature, use the **no** form of this command.

Syntax

clock summer-time *zone* **recurring** {**usa** | **eu** | {*week date month HH:MM week month date HH:MM*}} [**offset**]

clock summer-time *zone* **date** *month day year HH:MM month day year HH:MM* [**offset**]

no clock summer-time

Parameters

- *zone*—The acronym of the time zone to be displayed when the summer time is in effect. (Range: up to 4 characters)
- **recurring**—Specifies that the summer time starts and ends on the corresponding specified days every year.
  - **usa**—Specifies that the summer time rules are the United States rules.
  - **eu**—Specifies that the summer time rules are the European Union rules.
  - *week*—Number of the week in the month (1 to 4), first, or last.
  - *date*—Date of the week (first three characters by name, such as sun).
  - *month*—Month (first three characters by name, such as feb).
- **date**—Specifies that the summer time starts on the first date listed in the command and ends on the second date in the command.
  - *month*—Starting month (first three characters by name, such as feb).
  - *day*—Starting date. (Range: 1 to 31)
  - *year*—Starting date (no abbreviation). (Range: 2000 to 2037)
  - *HH:MM*—Starting time (military format) in hours and minutes. (Range: hh: 0 to 23, mm: 0 to 59)
- **offset**—(Optional) Number of minutes to add during the summer time. The default is 60 minutes. (Range: 1 to 1440)

Default Configuration

The summer time is disabled.

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 the 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 the standard time. The end time is relative to the summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

Example

```
switchxxxxxx(config)# clock summer-time abc date apr 1 2010 09:00 aug 2 2010
09:00
```

clock timezone

To set the time zone of the switch, use the **clock timezone** Global Configuration command.

To use the default time zone, use the **no** form of this command.

Syntax

clock timezone *zone HOUR-OFFSET* [*minutes*]

no clock timezone

Parameters

- *zone*—The acronym of the time zone. (Range: Up to 4 characters)
- *HOUR-OFFSET*—Hours difference from UTC. (Range: -12 to +13)
- *minutes*—(Optional) Minutes difference from UTC. (Range: 0 to 59)

Default Configuration

HOUR-Offset is +8. Acronym is DFL.

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.

Example

```
switchxxxxxx(config)# clock timezone abc +2 minutes 32
```

show time-range

Use the **show time-range** User EXEC mode command to display the time range configuration

Syntax

show time-range [*NAME*]

Parameters

- *NAME*—Name of time-range entry

Default Configuration

No default is defined.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show time-range** command to display time range entry settings.

Example

The following example shows how to show a time-range entry:

```
Switchxxxxxx# show time-range test
time-range entry: test (active)
absolute end 22:00 may 30 2015
periodic mon 18:00 to wed 22:00
periodic weekend 09:00 to 11:00
```

periodic

Use the **periodic** Time-range Configuration mode command to specify a recurring (weekly) time range for functions that support the time-range feature. Use the no form of this command to remove the time limitation.

Syntax

periodic (**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**) *HH:MM* **to** (**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**) *HH:MM*

no periodic (**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**) *HH:MM* **to** (**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**) *HH:MM*

periodic (**daily** | **weekdays** | **weekend**) *HH:MM* **to** *HH:MM*

periodic (**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**) | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] *HH:MM* to *HH:MM*

no periodic (**daily** | **weekdays** | **weekend**) *HH:MM* **to** *HH:MM*

no periodic (**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**) | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] | [(**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**)] *HH:MM* to *HH:MM*

Parameters

- **weekdays**—The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can be the following week (see description in the User Guidelines)..

- **hh:mm**—Time in hours and minutes.
- **daily** | **weekdays** | **weekend**—Specifies periodic range type .

Default Configuration

No default is defined.

Command Mode

Time-Range Configuration Mode

User Guidelines

Use the **periodic** command to set the periodic time of time range.

Use the **no** form of this command to remove periodic time.

You can verify your setting by entering the **show time-range Privileged EXEC** command

Example

The following example shows how to set periodic time:

```
switchxxxxxx (config)# time-range test
switchxxxxxx (config-time-range)# periodic mon 11:00 to fri 18:00
switchxxxxxx (config-time-range)# periodic wed 14:00 to fri 22:00
switchxxxxxx (config-time-range)# do show time-range test
time-range entry: test (active)
periodic mon 11:00 to fri 18:00
periodic wed 14:00 to fri 22:00

switchxxxxxx (config-time-range)# no periodic mon 11:00 to fri 18:00
switchxxxxxx (config-time-range)# do show time-range test
time-range entry: test (inactive)
periodic wed 14:00 to fri 22:00
```

show clock

To show the system time and date, use the **show clock** Privileged EXEC mode command.

Syntax

show clock [**detail**]

Parameters

- **detail**—(Optional) Displays the time zone and summer time configuration.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays the system time and date:

```
switchxxxxxx# show clock

08:11:18 abc(UTC+2:32) Mar 07 2012
Time source is sntp
```

Example 2—The following example displays the system time and date along with the time zone and the summer time configuration:

```
switchxxxxxx# show clock detail

08:11:44 abc(UTC+2:32) Mar 07 2012
Time source is sntp

Time zone:
Acronym is abc
Offset is UTC+2:32
```

show sntp configuration

To show the SNTP server defined on the switch, use the **show sntp configuration** Privileged EXEC mode command.

Syntax

show sntp configuration

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show sntp configuration
SNTP is Enabled
SNTP Server address: 192.1.1.1
SNTP Server port: 123
```

sntp server

To use SNTP to request and accept Network Time Protocol (NTP) traffic from a specific server (meaning to accept system time from an SNTP server), use the **sntp server** Global Configuration mode command.

To remove the SNTP server, use the **no** form of this command.

Syntax

sntp server {*ip-address* | *hostname*} [**port** *port-number*]

no sntp

Parameters

- *ip-address*—IPv4 address of the SNTP server.
- *hostname*—Hostname of the SNTP server. Only translation to IPv4 addresses is supported.
- **port** *port-number*—(Optional) Specifies the logical port number used for the SNTP client on the switch. The default is the well-known IANA port number for this service, 123. (Range: 1 to 65535)

Default Configuration

No SNTP servers are defined.

Command Mode

Global Configuration mode

Example

The following example configures the switch to accept SNTP traffic from the server on 192.1.1.1 with port 123:

```
switchxxxxxx(config)# sntp server 192.1.1.1 port 123
```

time-range

Use the **time-range** Global Configuration mode command to define time ranges different functions. In addition, this command enters the Time-range Configuration mode. All commands after this one refer to the time-range being defined.

Use the **no** form of this command to remove the time range from the device.

Syntax

time-range *NAME*

no time-range *NAME*

Parameters

- *NAME*—Name of time-range entry

Default Configuration

No default is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the **time-range** command to add time range entry.

Use the **no** form of this command to delete exist time range entry. Entry can't be reference by other features.

You can verify your setting by entering the **show time-range Privileged EXEC** command.

Example

The following example shows how to create and delete time-range entry:

```
switchxxxxxx (config)# time-range test
switchxxxxxx (config-time-range)# do show time-range test
time-range entry: test (active)

switchxxxxxx (config)# no time-range test
switchxxxxxx (config)# do show time-range test
```

9

Configuration and Image File Commands

boot host auto-config

To enable the DHCP Auto Configuration feature on the switch, use the **boot host auto-config** Global Configuration mode command.

To disable this feature on the switch, use the **no** form of this command.

Syntax

boot host auto-config

no boot host auto-config

Parameters

N/A

Default Configuration

DHCP Auto Configuration is enabled.

Command Mode

Global Configuration mode

User Guidelines

Auto Configuration enables passing configuration information to hosts on a TCP/IP network. Based on this protocol, the Auto Configuration feature enables a switch to download configuration files from a TFTP server. The switch can be configured as a DHCPv4 client in which auto configuration from a DHCPv4 server is supported or a DHCPv6 client in which auto configuration from a DHCPv6 server is supported.

After the switch obtains information such as configuration file name and TFTP server IP address from the DHCP server, it will first automatically download the specific configuration file from the remote TFTP server, copy the downloaded configuration to the startup configuration, and then reboot.

Example

```
switchxxxxxx(config)# boot host auto-config
```

boot system

To specify the active system image file that will be loaded at startup, use the **boot system** Global Configuration mode command.

Syntax

boot system {**image-1** | **image-2**}

Parameters

- **image-1**—Specifies that image1 will be loaded as the system image during the next startup.
- **image-2**—Specifies that image2 will be loaded as the system image during the next startup.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

The following example specifies image1 as the active system image file:

```
switchxxxxxx(config)# boot system image-1
Select "image1" Success
```

copy

To copy a source file to a destination file, use the **copy** Privileged EXEC mode command.

Syntax

copy

Parameters

The following table displays the file options:

Keyword	Source or Destination
backup-config	Backup configuration file. A configuration file can be downloaded to this file (without giving a file name). This can then be copied to the Running configuration file or the Startup configuration file.
flash://	Copy from the flash file system.
mirror-config	Mirror configuration file. If the Running configuration file and the Startup configuration file have been identical for 24 hours, the Startup configuration file is automatically copied to the Mirror Configuration file by the system. It can then be copied to the Startup configuration file or the Running configuration file if required.
running-config	Currently Running configuration file.
startup-config	Startup configuration file.
tftp://	Copy from a TFTP server. The syntax for this alias is **tftp://host/[directory]/filename**. The host can be either identified by an IP address or a hostname.

Command Mode

Privileged EXEC mode

User Guidelines

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

Copying a Configuration File from a Server

- Use the **copy tftp:// startup-config** command to copy a configuration file from a network server to the switch's Startup Configuration file.
- Use the **copy tftp:// running-config** command to copy a configuration file from a network server to the switch's Running Configuration file.
- Use the **copy tftp://backup-config** command to copy a configuration file from a network server to the switch's Backup Configuration file.

Storing a Configuration File on a Server

- Use the **copy running-config tftp://** command to copy the current Running Configuration file to a network server using TFTP.
- Use the **copy startup-config tftp://** command to copy the Startup Configuration file to a network server using TFTP.
- Use the **copy backup-config tftp://** command to copy the Backup Configuration file to a network server using TFTP.

Saving the Running Configuration to the Startup Configuration

- Use the **copy running-config startup-config** command to copy the Running Configuration file to the Startup Configuration file.

Backing Up the Running Configuration or Startup Configuration to the Backup Configuration

- Use the **copy running-config backup-config** command to copy the Running Configuration file to the Backup Configuration file.
- Use the **copy startup-config backup-config** command to copy the Startup Configuration file to the Backup Configuration file.

Restoring the Mirror Configuration File.

- Use **copy mirror-config startup-config** to copy the Mirror Configuration file to the Startup Configuration file.
- Use **copy mirror-config running-config** to copy the Mirror Configuration file to the Running Configuration file.

Examples

Example 1—The following example copies a system image file (file1) from the TFTP server 172.16.101.101 to the nonactive image file (image1):

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://image-1
Downloading file...Please Wait...
Upgrade firmware success. Do you want to reboot now? (y/n)
```

Example 2—The following example copies the Mirror Configuration file, saved by the system, to the Startup Configuration file:

```
switchxxxxxx# copy mirror-config startup-config
```

delete backup-config

To delete the Backup Configuration from the flash memory, use the **delete backup-config** Privileged EXEC mode command.

Syntax

delete backup-config

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example deletes the Backup Configuration file from the flash memory:

```
switchxxxxxx# delete backup-config
Delete backup-config [y/n]
```

delete startup-config

To delete the Startup Configuration from the flash memory, use the **delete startup-config** Privileged EXEC mode command. The system will start with the default configuration during the next startup.

Syntax

delete startup-config

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example deletes the Startup Configuration file from the flash memory:

```
switchxxxxxx# delete startup-config
Delete startup-config [y/n]
```

dir

To show information for the files in the flash memory, use the **dir** Privileged EXEC command.

Syntax

dir

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# dir
File Name           Flash Size      File Size       Modified
----------------------- --------------- --------------- --------------------
--
 startup-config           1245            1245            2000-01-01 08:05:03
 mirror-config            1245            1245            2000-01-02 10:32:01
 rsa2                     1679            1679            2000-01-01 08:00:37
 dsa2                     668             668             2000-01-01 08:00:48
 ssl_cert                 891             891             2000-01-01 08:01:08
 image-1                  13828096        7125944         2013-12-27 19:36:56
 image-2                  13828096        7141865         2014-01-10 17:44:55

Total size of flash: 32112640 bytes
Free size of flash: 4450720 bytes
```

ip dhcp tftp-server file

To set the full name of the configuration file located on the TFTP server, use the **ip dhcp tftp-server file** Global Configuration mode command.

To delete the configuration file setting, use the **no** form of this command.

Syntax

ip dhcp tftp-server file *WORD<1-128>*

no ip dhcp tftp-server file

Parameters

- *WORD<1-128>*—Full name of the configuration file located on the TFTP server defined in the **ip dhcp tftp-server ip address** command.

Default Configuration

No configuration file is specified.

Command Mode

Global Configuration mode

User Guidelines

This setting is only active when the DHCP options that the switch receives from the DHCP server do not include the TFTP server and configuration file information. In this case, the switch automatically downloads this configuration file from the TFTP server defined in the **ip dhcp tftp-server ip address** command.

Example

The following example specifies the backup configuration file name as autodhcp.cfg:

```
switchxxxxxx(config)# ip dhcp tftp-server file autodhcp.cfg
```

ip dhcp tftp-server ip address

To set the IP address or hostname of the TFTP server from which the switch can automatically download the configuration file by using the DHCP options, use the **ip dhcp tftp-server ip address** Global Configuration mode command.

To delete the TFTP server, use the **no** form of this command.

Syntax

ip dhcp tftp-server ip address {*ipv4-address* | *hostname* | *ipv6-address*}

no dhcp tftp-server ip address

Parameters

- *ipv4-address*—IPv4 address of the TFTP server.
- *hostname*—Hostname of the TFTP server.
- *ipv6-address*—IPv6 address of the TFTP server.

Default Configuration

No TFTP server is specified.

Command Mode

Global Configuration mode

User Guidelines

This setting is active only when the DHCP options that the switch receives from the DHCP server do not include the TFTP server and configuration file information. In this case, the switch automatically downloads the configuration file defined in the **ip dhcp tftp-server file** command from this TFTP server.

Example

```
switchxxxxxx(config)# ip dhcp tftp-server ip address autodhcp
```

management vlan ipv6 dhcp client information refresh

To set the refresh time and the minimum refresh time for DHCPv6 stateless client, use the **management vlan ipv6 dhcp client information refresh** Global Configuration mode command.

To use the default refresh time, use the **no** form of these commands.

Syntax

management vlan ipv6 dhcp client information refresh {*infinity*| *<86400-4294967294>*}

no management vlan ipv6 dhcp client information refresh

management vlan ipv6 dhcp client information refresh minimum {*infinity*| *<600-4294967294>*}

no management vlan ipv6 dhcp client information refresh minimum

Parameters

- *infinity*—The time never refreshes.
- *<86400-4294967294>*—The refresh time.
- <600-4294967294>—The minimum refresh time.

Default Configuration

The default refresh time is 86400 seconds.

The default minimum refresh time is 86400 seconds.

Command Mode

Global Configuration mode

User Guidelines

If the DHCPv6 server has an Information Refresh Time option in reply message, the switch use the refresh time defined by the DHCPv6 server, otherwise, the refresh time defined in this command is used.

However, if the refresh time defined by the DHCPv6 server is smaller than the minimum refresh time defined in this command, the switch uses the minimum refresh time defined in this command.

Example

The following example configures the refresh time and the minimum refresh time for DHCPv6 stateless client:

```
switchxxxxxx(config)# management vlan ipv6 dhcp client information refresh
115200
switchxxxxxx(config)# management vlan ipv6 dhcp client information refresh
minimum 115200
```

management vlan ipv6 dhcp client stateless

To enable the DHCPv6 stateless client, use the **management vlan ipv6 dhcp client stateless** Global Configuration mode command. This command will enable the DHCPv6 stateless client and send the information request to the DHCPv6 server.

To disable the DHCPv6 stateless client, use the **no** form of this command.

Syntax

management vlan ipv6 dhcp client stateless

no management vlan ipv6 dhcp client stateless

Parameters

N/A

Default Configuration

The DHCPv6 stateless client is disabled by default.

Command Mode

Global Configuration mode

Example

The following example enables the DHCPv6 stateless client on the switch:

```
switchxxxxxx(config)# management vlan ipv6 dhcp client stateless
```

renew dhcp force-autoconfig

To force the DHCP Auto Configuration procedure to be imitated, use the **renew dhcp force-autoconfig** Privileged EXEC mode command.

Syntax

renew dhcp force-autoconfig

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

After executing this command, the DHCP Auto Configuration procedure will start on the next DHCP renew for DHCPv4 and on the next information-request refresh for DHCPv6.

Example

```
switchxxxxxx# renew dhcp force-autoconfig
After auto config success, the original startup-config will be replaced and
system will reload.
Do you want to continue? (y/n)
```

show backup-config

To show information of the Backup Configuration file, use the **show backup-config** Privileged EXEC mode command.

Syntax

show backup-config

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

The Backup Configuration file does not contain all information that can be displayed in the output. Only nondefault settings are displayed.

Example

```
switchxxxxxx# show backup-config
config-file-header
Switch867001
v1.0.0.16
CLI v1.0
@
!
!
!
!
username "cisco" secret encrypted
ZmZmNzVhZTAzYjAyODkzZjlkM2JjZGIyMGYyMzY0NDM=
!
!
```

```
!
voice vlan oui-table add 00:E0:BB 3COM
voice vlan oui-table add 00:03:6B Cisco
voice vlan oui-table add 00:E0:75 Veritel
voice vlan oui-table add 00:D0:1E Pingtel
voice vlan oui-table add 00:01:E3 Siemens
voice vlan oui-table add 00:60:B9 NEC/Philips
voice vlan oui-table add 00:0F:E2 H3C
voice vlan oui-table add 00:09:6E Avaya
!
!
!
!
spanning-tree mst configuration
 name "00:E0:4C:86:70:01"
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface gi1
!
interface gi2
!
interface gi3
!
interface gi4
!
interface gi5
!
interface gi6
!
interface gi7
!
interface gi8
!
interface gi9
!
interface gi10
!
```

```
interface gi11
!
interface gi12
!
interface gi13
!
interface gi14
!
interface gi15
!
interface gi16
!
interface gi17
!
interface gi18
!
interface gi19
!
interface gi20
!
interface gi21
!
interface gi22
!
interface gi23
!
interface gi24
!
interface gi25
!
interface gi26
!
interface gi27
!
interface gi28
!
!
!

switchxxxxxx#
```

show boot

To show information of the DHCP Auto Configuration feature, use the **show boot** Privileged EXEC mode command.

Syntax

show boot

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx(config)# show boot
Auto Config
-----------
Config Download via DHCP: enabled
```

show bootvar

To show information of the system image file in the flash memory, use the **show bootvar** Privilege EXEC mode command.

Syntax

show bootvar

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show bootvar
Image  File Name   Version     Date                    Status
-----  ----------  ---------   --------------------    -----------
```

```
1       image-1        1.0.0.14      2014-02-07 09:32:39    Not active
2       image-2        1.0.0.16      2014-02-26 16:02:49    Active*

"*" designates that the image was selected for the next boot
```

show ip dhcp tftp-server

To show information about the active and user-defined TFTP servers, use the **show ip dhcp tftp-server** Privileged EXEC mode command.

Syntax

show ip dhcp tftp-server

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example shows information of the TFTP servers used for auto configuration through DHCP:

```
switchxxxxxx# show ip dhcp tftp-server
server address
active
manual
file path on server
active
manual
```

show running-config

To show the entire contents of the current Running Configuration file or show the contents of the Running Configuration file for specific interfaces, use the **show running-config** Privileged EXEC mode command.

Syntax

show running-config [**interfaces** *interface-list*]

Parameters

- **interfaces** *interface-list*—(Optional) Specifies an interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

The Running Configuration file does not contain all of the information that can be displayed in the output. Only nondefault settings are displayed.

Examples

Example 1—The following example shows the entire Running Configuration file:

```
switchxxxxx# show running-config
config-file-header
switchxxxxxx
v1.0.0.16
CLI v1.0
@
!
!
!
hostname "switchxxxxxx"
username "cisco" secret encrypted
ZmZmNzVhZTAzYjAyODkzZjlkM2JjZGIyMGYyMzY0NDM=
!
!
!
voice vlan oui-table add 00:E0:BB 3COM
voice vlan oui-table add 00:03:6B Cisco
voice vlan oui-table add 00:E0:75 Veritel
voice vlan oui-table add 00:D0:1E Pingtel
voice vlan oui-table add 00:01:E3 Siemens
```

```
voice vlan oui-table add 00:60:B9 NEC/Philips
voice vlan oui-table add 00:0F:E2 H3C
voice vlan oui-table add 00:09:6E Avaya
!
!
!
!
spanning-tree mst configuration
 name "00:E0:4C:86:70:01"
!
!
!
!
!
snmp-server
!
!
!
ip telnet server
ip ssh server
!
!
!
!
!
!
!
!
!
!
interface gi1
!
interface gi2
!
interface gi3
!
interface gi4
!
interface gi5
!
interface gi6
!
interface gi7
!
interface gi8
!
interface gi9
!
interface gi10
!
interface gi11
!
interface gi12
!
interface gi13
```

```
!
interface gi14
!
interface gi15
!
interface gi16
!
interface gi17
!
interface gi18
!
interface gi19
!
interface gi20
!
interface gi21
!
interface gi22
!
interface gi23
!
interface gi24
!
interface gi25
!
interface gi26
!
interface gi27
!
interface gi28
!
!
!
```

Example 2—The following example shows the Running Configuration file for fa2 and fa3:

```
switchxxxxxx# show running-config interfaces gi1-2
interface gi1
!
interface gi2
!
switchxxxxxx#
```

show startup-config

To show the contents of the Startup Configuration file, use the **show startup-config** Privileged EXEC mode command.

Syntax

show startup-config

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

The Startup Configuration file does not contain all information that can be displayed in the output. Only nondefault settings are displayed.

Example

```
switchxxxxxx# show startup-config
config-file-header
Switch867001
v1.0.0.16
CLI v1.0
@
!
!
!
!
username "cisco" secret encrypted
ZGZlYWYxMDM5MGU1NjBhZWE3NDVjY2JhNTNlMDQ0ZWQ=
!
!
!
voice vlan oui-table add 00:E0:BB 3COM
voice vlan oui-table add 00:03:6B Cisco
voice vlan oui-table add 00:E0:75 Veritel
voice vlan oui-table add 00:D0:1E Pingtel
voice vlan oui-table add 00:01:E3 Siemens
voice vlan oui-table add 00:60:B9 NEC/Philips
voice vlan oui-table add 00:0F:E2 H3C
voice vlan oui-table add 00:09:6E Avaya
!
!
!
```

```
!
spanning-tree mst configuration
 name "00:E0:4C:86:70:01"
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface gi1
!
interface gi2
!
interface gi3
!
interface gi4
!
interface gi5
!
interface gi6
!
interface gi7
!
interface gi8
!
interface gi9
!
interface gi10
!
interface gi11
!
interface gi12
!
interface gi13
!
interface gi14
!
interface gi15
!
interface gi16
!
```

```
interface gi17
!
interface gi18
!
interface gi19
!
interface gi20
!
interface gi21
!
interface gi22
!
interface gi23
!
interface gi24
!
interface gi25
!
interface gi26
!
interface gi27
!
interface gi28
!
!
!
```

write

To save the current Running Configuration to the Startup Configuration file, use the **write** Privileged EXEC mode command.

Syntax

write

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

```
switchxxxxxx# write
Building configuration...
[OK]
switchxxxxxx#
```

10

EEE Commands

eee enable (Interface)

To enable the EEE mode on an Ethernet interface, use the **eee enable** Interface Configuration mode command.

To disable the EEE mode on an Ethernet interface, use the **no** form of this command.

Syntax

eee enable

no eee enable

Parameters

N/A

Default Configuration

EEE is enabled.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# eee enable
Enabling or disabling EEE will cause the port first link down and then up.
Are you sure to proceed? [yes/no]:
```

11

Ethernet Configuration Commands

clear counters

To clear the statistics counters on all interfaces or on a specific interface, use the **clear counters** Privileged EXEC Mode command.

Syntax

clear counters [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface ID can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

The following example clears the statistics counters for gi5:

```
switchxxxxxx# clear counters interfaces gi5
```

clear etherlike statistics

To clear the Etherlike statistics counters on all interfaces, use the **clear etherlike statistics** Privileged EXEC Mode command.

Syntax

clear etherlike statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# clear etherlike statistics
```

default interface

To restore an interface to its default settings, use the **default interface** Interface Configuration mode command.

Syntax

default interface *interface-id*

Parameters

- *interface-id*—The Ethernet interface ID.

Default Configuration

N/A

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# default interface gi1
Interface gi1 set to default configuration
```

description

To add a description to an interface, use the **description** Interface Configuration mode command.

To delete the description of an interface, use the **no** form of this command.

Syntax

description *string*

no description

Parameters

- *string*—The description of an interface. (Length: 0 to 32 characters)

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# description SW#3
```

duplex

To configure the full or half duplex operation for a given Ethernet interface when not using auto-negotiation, use the **duplex** Interface Configuration mode command.

Syntax

duplex {**half** | **full** | **auto**}

Parameters

- **half**—Forces the half-duplex operation.
- **full**—Forces the full-duplex operation.
- **auto**—Enables auto-duplex configuration.

Default Configuration

The interface operates in the full-duplex mode.

Command Mode

Interface Configuration (port channel) mode

Example

The following example configures gi5 to operate in the full-duplex mode:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# duplex full
```

errdisable recovery

To enable errdisable recovery from specific causes and set the recovery interval, use the **errdisable recovery** Global Configuration command.

To revert to its default setting, use the **no** form of this command.

Syntax

errdisable recovery {**cause** {**all** | **acl** | **arp-inspection** | **bpduguard** | **broadcast-flood** | **dot1x-src-address** | **dhcp-rate-limit** | **inline-power** | **loopback-detection** | **psecure-violation** | **selfloop** | **unicast-flood** | **unknown-multicastflood**} | **interval** *interval*}

no errdisable recovery {**cause** {**all** | **acl** | **arp-inspection** | **bpduguard** | **broadcast-flood** | **dot1x-src-address** | **dhcp-rate-limit** | **inline-power** | **loopback-detection** | **psecure-violation** | **selfloop** | **unicast-flood** | **unknown-multicastflood**}

Parameters

- **cause**—Enables errdisable recovery from a specific cause. The available options are:
  - **all**—Enables the timer to recover from all causes.
  - **acl**—Enables the timer to recover from the ACL causes.
  - **arp-inspection**—Enables the timer to recover from the ARP inspection causes.
  - **bpduguard**—Enables the timer to recover from the BPDU Guard causes.
  - **broadcast-flood**—Enables the timer to recover from the flood causes.
  - **dhcp-rate-limit**—Enables the timer to recover from the DHCP rate limit causes.
  - **dot1x-src-address**—Enables the timer to recover from the 802.1X single host mode violation causes.
  - **inline-power**—Enables the timer to recover from the inline-power causes.
  - **loopback-detection**—Enables the timer to recover from the loopback-detection causes.
  - **psecure-violation**—Enables the timer to recover from the port security causes.
  - **selfloop**—Enables the timer to recover from the self-loop causes.
  - **unicast-flood**—Enables the timer to recover from the unicast flood causes.
  - **unknown-multicast-flood**—Enables the timer to recover from the unknown multicast flood causes.

- **interval** *interval*—Specifies the time to recover from a specific error-disable state. The same interval is applied to all causes. (Range: 30 to 86400 seconds, default: 300 seconds)

Default Configuration

Errdisable recovery is disabled for all causes.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# errdisable recovery cause all
switchxxxxxx(config)# errdisable recovery interval 64
```

flowcontrol

To configure flow control on a given interface, use the **flowcontrol** Interface Configuration mode command.

To disable flow control on an interface, use the **no** form of this command.

Syntax

flowcontrol {**auto** | **on** | **off**}

no flowcontrol

Parameters

- **auto**—Automatically enables or disables flow control on the interface.
- **on**—Enables flow control on the interface.
- **off**—Disables flow control on the interface.

Default Configuration

Flow control is disabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# flowcontrol on
```

interface

To enter the Interface Configuration mode in order to configure an interface, use the **interface** Global Configuration mode command.

Syntax

interface *interface-id*

Parameters

- *interface-id*—The interface ID can be one of these types: Ethernet port, port channel, VLAN, range, IP interface, or tunnel.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, port channel, VLAN, Range) mode

Examples

Example 1—The following example enters the Interface Configuration mode in order to configure a Gigabit Ethernet port:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)#
```

Example 2—The following example enters the Interface Configuration mode in order to configure a Fast Ethernet port:

```
switchxxxxxx(config)# interface fa1
switchxxxxxx(config-if)#
```

Example 3 - The following example enters the Interface Configuration mode in order to configure a port channel (LAG):

```
switchxxxxxx(config)# interface po1
switchxxxxxx(config-if)#
```

interface range

To execute a command on multiple interfaces simultaneously, use the **interface range** command.

Syntax

interface range *interface-list*

Parameters

- *interface-list*—A list of interface IDs. The interface ID can be one of these types: Ethernet port, VLAN, or port channel.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, port channel, or VLAN) mode

User Guidelines

The commands under the interface range are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Example

```
switchxxxxxx(config)# interface range gi1-20
switchxxxxxx(config-if-range)#
```

jumbo-frame

To enable jumbo frames on the switch and set the maximum frame size supported by the switch, use the **jumbo-frame** Global Configuration mode command.

To disable jumbo frames on the switch, use the **no** form of this command.

Syntax

jumbo-frame *frame-size*

no jumbo-frame

Parameters

- *frame-size*—Maximum size of packet in bytes that the switch can support. (Range: 1518 to 10000 bytes, default: 1522 bytes)

Default Configuration

Jumbo frames are disabled on the switch.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the switch.

Example

The following example enables jumbo frames on the switch and sets the maximum frame size to 1538 bytes:

```
switchxxxxxx(config)# jumbo-frame 1538
```

operation time-range

To control the time that the port is up, use the **operation time-range** Interface Configuration mode command. To cancel the time range for the port operation time, use the no form of this command.

Syntax

operation time-range *NAME*

no operation time-range

Parameters

- *NAME*—Specify the name of time-range settings. (Range: 1–32 characters.)

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, Port Channel) mode

User Guidelines

Use the **operation time-range** *NAME* command to bind a time-range profile to interfaces. Use the **no operation time-range** to reset the time-range.

Example

The following example shows how to apply the workhour time-range to an interface and how to verify the configuration:

```
Switch(config)# interface fa1
Switch(config-if)# operation time-range workhour

Switch(config-if)# do show interface status fa1

Port  Name       Status      Vlan  Duplex  Speed    Type
fa1              connected   1     a-full  a-100M   Copper

Port Working Time Range               Status
---- -------------------------------- --------
fa1  workhour                         Active
```

show errdisable recovery

To show the error-disable recovery status and the interfaces in the error-disabled state, use the **show errdisable recovery** Privileged EXEC Mode command.

Syntax

show errdisable recovery

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show errdisable recovery
ErrDisable Reason          | Timer Status
---------------------------+---------------
                 bpduguard | disabled
                  selfloop | disabled
           broadcast-flood | disabled
  unknown-multicast-flood | disabled
             unicast-flood | disabled
                       acl | disabled
         psecure-violation | disabled
           dhcp-rate-limit | disabled
            arp-inspection | disabled

Timer Interval : 300 seconds


Interfaces that will be enabled at the next timeout:

Port |  Error Disable Reason    | Time Left
-----+--------------------------+------------
```

show interface status

To show the status for all interfaces or for a specific interface, use the **show interface status** Privileged EXEC Mode command.

Syntax

show interface status [*interface-id*]

Parameters

- *interface-id*—The interface ID or a list of interface IDs. The interface ID can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC Mode

Default Configuration

N/A

Example

```
switchxxxxxx# show interfaces status gi1-10
Port  Name                 Status       Vlan  Duplex  Speed    Type
gi1                        notconnect   1     auto    auto     Copper
gi2                        notconnect   1     auto    auto     Copper
gi3                        notconnect   1     auto    auto     Copper
gi4                        notconnect   1     auto    auto     Copper
gi5   swx3                 notconnect   1     auto    auto     Copper
gi6                        notconnect   1     auto    auto     Copper
gi7                        notconnect   1     auto    auto     Copper
gi8                        notconnect   1     auto    auto     Copper
gi9                        notconnect   1     auto    auto     Copper
gi10                       connected    1     a-full  a-1000M  Copper

Port Time Range              Status
---- ------------------------------- --------
gi1
gi2
gi3
gi4  Weekend                Inactive
gi5
gi6
gi7
gi8  Weekday                Active
gi9
gi10
```

show storm-control

To show the storm control settings for all interfaces or for a specific interface, use the **show storm-control** Privileged EXEC mode command.

Syntax

show storm-control [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface ID can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show storm-control
Storm control preamble and IFG: Excluded
  Storm control unit: bps

  Port    | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |
Action
        |       |     kbps    |        kbps        |      kbps       |
----------+-------+-------------+--------------------+-----------------|----
-------
  gi1      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi2      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi3      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi4      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi5      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi6      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi7      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi8      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
```

```
  gi9      disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi10     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi11     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi12     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi13     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi14     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi15     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi16     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi17     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi18     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi19     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi20     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi21     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi22     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi23     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi24     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi25     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi26     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi27     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
  gi28     disable Off(  10000)   Off(  10000)         Off(  10000)
Drop
```

shutdown

To disable an interface, use the **shutdown** Interface Configuration mode command.

To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Parameters

N/A

Default Configuration

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Examples

Example 1—The following example disables the Ethernet port gi5:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# shutdown
```

Example 2—The following example restarts the disabled Ethernet port gi5:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# no shutdown
```

speed

To configure the speed for a given Ethernet interface when not using auto-negotiation, use the **speed** Interface Configuration mode command.

Syntax

speed {**10** | **100** | **1000** | **auto**}

Parameters

- **10—**Enables 10-Mbps operation.
- **100—**Enables 100-Mbps operation.

- **1000**—Enables 1000-Mbps operation.
- **Auto**—Enables auto speed configuration. The port automatically detects the speed at which it should run at based on the port at the other end of the link. If you use the 10, 100, or 1000 keywords with the auto keyword, the port only auto-negotiates at the specified speed.

Default Configuration

The port operates at its maximum speed capability.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

For 10/100-Mbps ports, if both speed and duplex are set to specific values, the link operates at the negotiated speed and duplex value.

For 10/100/1000-Mbps ports, if both the speed and duplex are set to specific values, autonegotiation is disabled.

You can configure the Fast Ethernet port speed as either 10 or 100 Mbps. You cannot configure the speed on the SFP module ports, but you can configure the speed to not negotiate (nonegotiate) if it is connected to a device that does not support autonegotiation. However, when a 1000BASE-T SFP module is inserted into the SFP module port, you can configure the speed as 10, 100, 1000 Mbps, or auto.

If the speed is set to auto, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend that you use the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, you must manually configure the duplex and speed settings on the other side.

Example

The following example configures the speed of fa5 to 100 Mbps:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# speed 100
```

storm-control action

To set the action when the received storm control packets exceed the maximum rate on an interface, use the **storm-control action** Interface Configuration mode command.

To disable the storm control action, use the **no** form of this command.

Syntax

storm-control action {**drop** | **shutdown**}

no storm-control action

Parameters

- **drop**—Drops incoming packets when the received packets exceed the maximum rate on an interface.
- **shutdown**—Shuts down the interface when the received packets exceed the maximum rate on an interface.

Default Configuration

The default action is **drop**.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# storm-control action drop
```

storm-control broadcast

To enable storm control of broadcast traffic on an interface, use the **storm-control broadcast** Interface Configuration mode command.

To disable storm control of broadcast traffic, use the **no** form of this command.

Syntax

storm-control broadcast

no storm-control broadcast

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface fa5
switchxxxxxx(config-if)# storm-control broadcast
```

storm-control broadcast level

To configure the maximum rate of broadcast traffic on an interface, use the **storm-control broadcast level** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

storm-control broadcast level {*pps* | *kbps*}

no storm-control broadcast level

Parameters

- {*pps* | *kbps*}—Specifies the maximum rate of broadcast traffic on a port. The unit of this rate depends on the settings in the **storm-control unit** command. (Range: 1 to 262134 pps or 16 to 1000000 kbps)

Default Configuration

10000

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Use the **storm-control broadcast level** command to enable storm control of broadcast traffic on an interface.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# storm-control broadcast level 12345
```

storm-control enable

To enable storm control on an interface, use the **storm-control enable** Interface Configuration mode command.

To disable storm control, use the **no** form of this command.

Syntax

storm-control enable

no storm-control enable

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# storm-control enable
```

storm-control ifg

To set the interframe configuration of storm control counting, use the **storm-control ifg** Global Configuration command.

Syntax

storm-control ifg {**include** | **exclude**}

Parameters

- **include**—Includes preamble and IFG.
- **exclude**—Excludes preamble and IFG.

Default Configuration

Exclude

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# storm-control ifg include
```

storm-control unit

To set the unit of storm control counting, use the **storm-control unit** Global Configuration command.

Syntax

storm-control unit {**bps** | **pps**}

Parameters

- **bps**—Specifies the unit as bits per second.
- **pps**—Specifies the unit as packets per second.

Default Configuration

The default is bps.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# storm-control unit pps
```

storm-control unknown-multicast

To enable storm control for unknown multicast traffic on an interface, use the **storm-control unknown-multicast** Interface Configuration mode command.

To disable storm control for unknown multicast traffic, use the **no** form of this command.

Syntax

storm-control unknown-multicast

no storm-control unknown-multicast

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# storm-control unknown-multicast
```

storm-control unknown-multicast level

To configure the maximum rate of unknown multicast traffic on an interface, use the **storm-control unknown-multicast level** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

storm-control unknown-multicast level {*pps* | *kbps*}

no storm-control unknown-multicast level

Parameters

- {*pps* | *kbps*}—Specifies the maximum rate of unknown multicast traffic on an interface. The unit of this rate depends on the settings in the **storm-control unit** Global Configuration mode command. (Range: 1 to 262134 pps or 16 to 1000000 kbps)

Default Configuration

10000

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Use the **storm-control unknown-multicast level** Interface Configuration mode command to enable storm control of unknown multicast traffic on an interface.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# storm-control unknown-multicast level 12345
```

storm-control unknown-unicast

To enable storm control for unknown unicast traffic on an interface, use the **storm-control unknown-unicast** Interface Configuration mode command.

To disable storm control for unknown unicast traffic, use the **no** form of this command.

Syntax

storm-control unknown-unicast

no storm-control unknown-unicast

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# storm-control unknown-unicast
```

storm-control unknown-unicast level

To configure the maximum rate of unknown unicast traffic on an interface, use the **storm-control unknown-unicast level** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

storm-control unknown-unicast level {*pps* | *kbps*}

no storm-control unknown-unicast level

Parameters

- {*pps* | *kbps*}—Specifies the maximum rate of unknown unicast traffic on an interface. The unit of this rate depends on the settings in the **storm-control unit** Global Configuration mode command. (Range: 1 to 262134 pps or 16 to 1000000 kbps)

Default Configuration

10000

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Use the **storm-control unknown-unicast level** Interface Configuration command to enable storm control for unknown unicast traffic on an interface.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Example

```
switchxxxxxx(config)# interface fa1
switchxxxxxx(config-if)# storm-control unknown-unicast level 12345
```

12

GVRP Commands

clear gvrp statistics

To clear Generic VLAN Registration Protocol (GVRP) statistics for all interfaces or for an interface, use the **clear gvrp statistics** Privileged EXEC command.

Syntax

clear gvrp {**error-statistics** | **statistics**} [**interfaces** *interface-id*]

Parameters

- **error-statistics**—Clears error statistics only.
- **statistics**—Clears normal statistics.
- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface must be an Ethernet port.

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# clear gvrp statistics interfaces gi11
```

gvrp enable (Global)

To enable GVRP globally on the switch, use the **gvrp enable** Global Configuration mode command.

To disable GVRP on the switch, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Parameters

N/A

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# gvrp enable
```

gvrp enable (Interface)

To enable GVRP on an interface, use the **gvrp enable** Interface Configuration mode command.

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.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member of a single VLAN. Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN ID.

Example

```
switchxxxxxx(config)# interface gi6
switchxxxxxx(config-if)# gvrp enable
```

gvrp registration-mode

To deregister all dynamic VLANs on an interface and prevent VLAN creation or registration on the interface, use the **gvrp registration-mode** Interface Configuration mode command.

Syntax

gvrp registration-mode {**fixed** | **forbidden** | **normal**}

Parameters

- **fixed**—Specifies the fixed mode.
- **forbidden**—Specifies the forbidden mode.
- **normal**—Specifies the normal mode.

Default Configuration

Normal mode

Command Mode

Interface Configuration (Ethernet, Port Channel) mode

Example

The following example forbids dynamic VLAN registration on fa2:

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# gvrp registration-mode forbidden
```

gvrp vlan-creation-forbid

To disable dynamic VLAN creation or modification, use the **gvrp vlan-creation-forbid** Interface Configuration mode command.

To enable dynamic VLAN creation or modification, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Parameters

N/A

Default Configuration

Dynamic VLAN creation is enabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# gvrp vlan-creation-forbid
```

show gvrp

To show the GVRP configuration, use the **show gvrp** Privileged EXEC mode command.

Syntax

show gvrp

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show gvrp
                GVRP    Status
                --------------------
    GVRP                            : Disabled
    Join time                       : 200 ms
    Leave time                      : 600 ms
    LeaveAll time                   : 10000 ms
```

show gvrp configuration

To show the GVRP configuration on specific interfaces, use the **show gvrp configuration** Privileged EXEC mode command.

Syntax

show gvrp configuration [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the GVRP configuration on all interfaces:

```
switchxxxxxx# show gvrp configuration
Port   |  GVRP-Status  | Registration  | Dynamic VLAN Creation
-------+---------------+---------------+----------------------
 gi1             Disabled          Normal               Enabled
 gi2             Disabled          Normal               Enabled
 gi3             Disabled          Normal               Enabled
 gi4             Disabled          Normal               Enabled
 gi5             Disabled          Normal               Enabled
 gi6             Disabled          Normal               Enabled
 gi7             Disabled          Normal               Enabled
 gi8             Disabled          Normal               Enabled
 gi9             Disabled          Normal               Enabled
gi10             Disabled          Normal               Enabled
gi11             Disabled          Normal               Enabled
gi12             Disabled          Normal               Enabled
gi13             Disabled          Normal               Enabled
gi14             Disabled          Normal               Enabled
gi15             Disabled          Normal               Enabled
gi16             Disabled          Normal               Enabled
gi17             Disabled          Normal               Enabled
gi18             Disabled          Normal               Enabled
gi19             Disabled          Normal               Enabled
gi20             Disabled          Normal               Enabled
gi21             Disabled          Normal               Enabled
gi22             Disabled          Normal               Enabled
gi23             Disabled          Normal               Enabled
gi24             Disabled          Normal               Enabled
gi25             Disabled          Normal               Enabled
gi26             Disabled          Normal               Enabled
gi27             Disabled          Normal               Enabled
gi28             Disabled          Normal               Enabled
 po1             Disabled          Normal               Enabled
 po2             Disabled          Normal               Enabled
 po3             Disabled          Normal               Enabled
 po4             Disabled          Normal               Enabled
 po5             Disabled          Normal               Enabled
 po6             Disabled          Normal               Enabled
 po7             Disabled          Normal               Enabled
 po8             Disabled          Normal               Enabled
```

show gvrp error-statistics

To show the GVRP error statistics for all interfaces or for a specific interface, use the **show gvrp error-statistics** Privileged EXEC mode command.

Syntax

show gvrp error-statistics [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interfaces. The interfaces can be one of these types: Ethernet port or port channel. If no interface ID is specified, GVRP error statistics for all interfaces are displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show gvrp error-statistics
Legend:
INVPROT : Invalid protocol Id
INVATYP : Invalid Attribute Type   INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value  INVEVENT: Invalid Event
  Port   | INVPROT | INVATYP | INVALEN | INVAVAL | INVEVENT
   gi1           0         0         0         0         0
   gi2           0         0         0         0         0
   gi3           0         0         0         0         0
   gi4           0         0         0         0         0
   gi5           0         0         0         0         0
   gi6           0         0         0         0         0
   gi7           0         0         0         0         0
   gi8           0         0         0         0         0
   gi9           0         0         0         0         0
  gi10           0         0         0         0         0
  gi11           0         0         0         0         0
  gi12           0         0         0         0         0
  gi13           0         0         0         0         0
  gi14           0         0         0         0         0
  gi15           0         0         0         0         0
  gi16           0         0         0         0         0
  gi17           0         0         0         0         0
  gi18           0         0         0         0         0
```

```
gi19            0          0          0          0          0
gi20            0          0          0          0          0
gi21            0          0          0          0          0
gi22            0          0          0          0          0
gi23            0          0          0          0          0
gi24            0          0          0          0          0
gi25            0          0          0          0          0
gi26            0          0          0          0          0
gi27            0          0          0          0          0
gi28            0          0          0          0          0
 po1            0          0          0          0          0
 po2            0          0          0          0          0
 po3            0          0          0          0          0
 po4            0          0          0          0          0
 po5            0          0          0          0          0
 po6            0          0          0          0          0
 po7            0          0          0          0          0
 po8            0          0          0          0          0
```

show gvrp statistics

To show the GVRP statistics for all interfaces or for a specific interface, use the **show gvrp statistics** Privileged EXEC mode command.

Syntax

show gvrp statistics [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interfaces. The interfaces can be one of these types: Ethernet port or port channel. If no interface ID is specified, GVRP statistics for all interfaces are displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show gvrp statistics
Port id         : fa1
```

```
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          : fa2
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          :  fa3
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          :  fa4
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
```

```
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          :  fa5
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0


Port id          :  fa6
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          :  fa7
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
```

```
LeaveAll TX     :    0

Port id         :  fa8
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         :  fa9
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa10
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa11
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
```

```
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa12
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa13
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa14
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
```

```
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa15
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa16
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa17
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa18
Total RX        :    0
JoinEmpty RX    :    0
```

```
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa19
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa20
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa21
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
```

```
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa22
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa23
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         : fa24
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0

Port id         :  gi1
```

```
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0

Port id           :  gi2
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0

Port id           :  po1
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0

Port id           :  po2
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
```

```
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0

Port id           :  po3
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0

Port id           :  po4
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0

Port id           :  po5
Total RX          :    0
JoinEmpty RX      :    0
JoinIn RX         :    0
Empty RX          :    0
LeaveIn RX        :    0
LeaveEmpty RX     :    0
LeaveAll RX       :    0
Total TX          :    0
JoinEmpty TX      :    0
JoinIn TX         :    0
Empty TX          :    0
LeaveIn TX        :    0
LeaveEmpty TX     :    0
LeaveAll TX       :    0
```

```
Port id          :  po6
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          :  po7
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0

Port id          :  po8
Total RX         :    0
JoinEmpty RX     :    0
JoinIn RX        :    0
Empty RX         :    0
LeaveIn RX       :    0
LeaveEmpty RX    :    0
LeaveAll RX      :    0
Total TX         :    0
JoinEmpty TX     :    0
JoinIn TX        :    0
Empty TX         :    0
LeaveIn TX       :    0
LeaveEmpty TX    :    0
LeaveAll TX      :    0
```

13

IGMP Snooping Commands

clear ip igmp snooping groups

To delete the Internet Group Management Protocol (IGMP) group cache entries, use the **clear ip igmp snooping groups** Privileged EXEC mode command.

Syntax

clear ip igmp snooping groups [**dynamic** | **static**]

Parameters

- **dynamic**—(Optional) Deletes dynamic group entries.
- **static**—(Optional) Deletes static group entries.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip igmp snooping groups
```

clear ip igmp snooping statistics

To clear the IGMP Snooping statistics, use the **clear ip igmp snooping statistics** Privileged EXEC mode command.

Syntax

clear ip igmp snooping statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip igmp snooping statistics
```

ip igmp filter

To control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface, use the **ip igmp filter** Interface Configuration mode command.

To remove an IGMP profile from the interface, use the **no** form of this command.

Syntax

ip igmp filter *profile-number*

no ip igmp filter

Parameter

- *profile-number*—The IGMP profile number to be applied. (Range: 1 to 128)

Default Configuration

No IGMP profiles are applied.

Command Mode

Interface Configuration mode

User Guidelines

An IGMP profile can be applied to one or more interfaces, but one interface can have only one profile applied to it.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ip igmp filter 22
```

ip igmp max-groups

To set the maximum number of IGMP groups that an interface can join or to configure the IGMP throttling action when the maximum number of entries in the forwarding table is reached, use the **ip igmp max-groups** Interface Configuration mode command.

To set the maximum number of IGMP groups back to the default (no maximum limit) or to return to the default throttling action (the report is dropped), use the **no** form of this command.

Syntax

ip igmp max-groups *number*

no ip igmp max-groups

ip igmp max-groups action {**deny** | **replace**}

Parameters

- *number*—The maximum number of IGMP groups that an interface can join.
- **action deny**—Drops the next IGMP join report when the maximum number of entries in the IGMP Snooping forwarding table is reached. This is the default action.
- **action replace**—Replaces the existing group with the new group for which the IGMP report was received when the maximum number of entries in the IGMP Snooping forwarding table is reached.

Command Mode

Interface Configuration mode

User Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries in the forwarding table is reached, the switch drops the next IGMP report received on the interface.
- If you configure the throttling action as replace and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries in the forwarding table is reached, the switch replaces a randomly selected multicast entry with the received IGMP report.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ip igmp max-groups 25
switchxxxxxx(config-if)# ip igmp max-groups action replace
```

ip igmp profile

To create an IGMP profile and enter the IGMP Profile Configuration mode, use the **ip igmp profile** Global Configuration mode command. From this mode, you can specify the settings of the IGMP profile to be used for filtering IGMP membership reports from a switch port.

To delete an IGMP profile, use the **no** form of this command.

Syntax

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

Parameters

- *profile-number*—The IGMP profile number. (Range: 1 to 128)

Default Configuration

No IGMP profiles are defined.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip igmp profile 20
switchxxxxxx(config-igmp-profile)#
```

ip igmp snooping

To enable IGMP Snooping on the switch, use the **ip igmp snooping** Global Configuration mode command.

To disable IGMP Snooping on the switch, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Parameters

N/A

Default Configuration

IGMP Snooping is enabled by default.

Command Mode

Global Configuration mode

Example

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

ip igmp snooping version

To configure the IGMP Snooping version, use the **ip igmp snooping version** Global Configuration mode command.

Syntax

ip igmp snooping version {**2** | **3**}

Parameters

- **version 2** —Specifies the IGMP version as IGMPv2.
- **version 3**—Specifies the IGMP version as IGMPv3.

Default Configuration

IGMPv2

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip igmp snooping version 3
```

ip igmp snooping report-suppression

To enable IGMP Snooping report suppression, use the **ip igmp snooping report-suppression** Global Configuration mode command.

To disable IGMP Snooping report suppression and forward all IGMP reports to multicast routers, use the **no** form of this command.

Syntax

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Parameters

N/A

Default Configuration

IGMP Snooping report suppression is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

IGMP Snooping report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP Snooping report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled, the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to the multicast routers.

Example

```
switchxxxxxx(config)# ip igmp snooping report-suppression
```

ip igmp snooping unknown-multicast action

To set the action when the switch receives an unknown multicast packet, use the **ip igmp snooping unknown-multicast action** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping unknown-multicast action {**drop** | **flood** | **router-port**}

no ip igmp snooping unknown-multicast action

Parameters

- **drop**—Drops all unknown multicast packets.
- **flood**—Floods all unknown multicast packets to ports in the same VLAN.
- **router-port**—Sends all unknown multicast packets to the router port.

Default Configuration

The default is **flood**.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip igmp snooping unknown-multicast action drop
```

ip igmp snooping vlan

To enable IGMP Snooping on specific VLANs, use the **ip igmp snooping vlan** Global Configuration mode command.

To disable IGMP Snooping on specific VLANs, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST*

no ip igmp snooping vlan *VLAN-LIST*

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)

Default Configuration

IGMP Snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

IGMPv1, IGMPv2, and IGMPv3 are supported.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

ip igmp snooping vlan immediate-leave

To enable the IGMP Snooping immediate leave processing on a VLAN, use the **ip igmp snooping vlan immediate-leave** Global Configuration mode command.

To disable IGMP Snooping immediate leave processing, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **immediate-leave**

no ip igmp snooping vlan *VLAN-LIST* **immediate-leave**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)

Default Configuration

IGMP Snooping immediate leave is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

ip igmp snooping vlan forbidden mrouter

To forbid a port from being defined as a multicast router port by static configuration or by automatic learning, use the **ip igmp snooping vlan forbidden mrouter** Global Configuration mode command.

To remove the configuration, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **forbidden mrouter interfaces** *interface-id*

no ip igmp snooping vlan *VLAN-LIST* **forbidden mrouter interfaces** *interface-id*

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No ports are defined.

Command Mode

Global Configuration mode

User Guidelines

A port that is a forbidden Mrouter port cannot be a multicast router port (for example, cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden mrouter interfaces
gi1
```

ip igmp snooping vlan forbidden forward-all

To enable the IGMP Snooping forbidden forward-all port processing on a VLAN, use the **ip igmp snooping vlan forbidden forward-all** Global Configuration mode command.

To disable this feature, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **forbidden forward-all interfaces** *interface-id*

no ip igmp snooping vlan *VLAN-LIST* **forbidden forward-all interfaces** *interface-id*

Parameter

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No port is configured as a member of a multicast group.

Command Mode

Global Configuration mode

User Guidelines

All registered multicast entries will always remove the forbidden forward-all.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden forward-all
interfaces fa11
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden forward-all
interfaces gi1
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden forward-all
interfaces po1
```

ip igmp snooping vlan last-member-query-count

To configure the last member query counter on a VLAN, use the **ip igmp snooping vlan last-member-query-count** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **last-member-query-count** *count*

no ip igmp snooping vlan *VLAN-LIST* **last-member-query-count**

Parameter

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- *count* —The number of times that group-specific or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1 to 7)

Default Configuration

2

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config-if)# ip igmp snooping vlan 3 last-member-query-count 7
```

ip igmp snooping vlan last-member-query-interval

To configure the last member query interval on a VLAN, use the **ip igmp snooping vlan last-member-query-interval** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **last-member-query-interval** *seconds*

no ip igmp snooping vlan *VLAN-LIST* **last-member-query-interval**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- *seconds*—The interval in seconds at which IGMP group-specific host query messages are sent on the interface. (Range: 1 to 25)

Default Configuration

1

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 3 last-member-query-interval 2
```

ip igmp snooping vlan mrouter

To enable automatic learning of multicast router ports on a VLAN, use the **ip igmp snooping vlan mrouter** Global Configuration mode command.

To remove the configuration, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **mrouter learn pim-dvmrp**

no ip igmp snooping vlan *VLAN-LIST* **mrouter learn pim-dvmrp**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)

Default Configuration

Learning pim-dvmrp is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports are learned according to:

- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

ip igmp snooping vlan querier

To enable the IGMP querier on specific VLANs, use the **ip igmp snooping vlan querier** Global Configuration mode command.

To disable the IGMP querier on specific VLANs, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier**

no ip igmp snooping vlan *VLAN-LIST* **querier**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

When the IGMP Snooping querier is enabled, it starts after a quarter of operation query-interval with no IGMP traffic being detected from a multicast router.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```

ip igmp snooping vlan querier version

To configure the IGMP version for an IGMP querier on specific VLANs, use the **ip igmp snooping vlan querier version** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier version** {**2** | **3**}

no ip igmp snooping vlan *VLAN-LIST* **querier version**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- **querier version 2**—The IGMP version is IGMPv2.
- **querier version 3**—The IGMP version is IGMPv3.

Default Configuration

The default IGMP version is IGMPv2.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

ip igmp snooping vlan query-interval

To set the query interval on a VLAN, use the **ip igmp snooping vlan query-interval** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **query-interval** *seconds*

no ip igmp snooping vlan *VLAN-LIST* **query-interval**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- *seconds*—The frequency in seconds at which IGMP query messages are sent on the interface. (Range: 30 to 18000)

Default Configuration

The default IGMP query interval is 125 seconds.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 3 query-interval 50
```

ip igmp snooping vlan response-time

To configure the maximum query response time on a VLAN, use the **ip igmp snooping vlan response-time** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **response-time** *seconds*

no ip igmp snooping vlan *VLAN-LIST* **response-time**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- *seconds*—Maximum response time in seconds advertised in IGMP queries. (Range: 5 to 20)

Default Configuration

10

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 3 response-time 20
```

ip igmp snooping vlan robustness-variable

To set the IGMP robustness variable on a VLAN, use the **ip igmp snooping vlan robustness-variable** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **robustness-variable** *count*

no ip igmp snooping vlan *VLAN-LIST* **robustness-variable**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- *count*—The number of expected packet loss on a link. (Range:1 to 7)

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# interface vlan 1 robustness-variable 5
```

ip igmp snooping vlan static

To enable the IGMP Snooping static group processing on a VLAN, use the **ip igmp snooping vlan static** Global Configuration mode command.

To disable this feature, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **static** *IPv4-Addr* **interface** *interface-id*

no ip igmp snooping vlan *VLAN-LIST* **static** *IPv4-Addr* **interface** *interface-id*

Parameter

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- *IPv4-Addr*—IPv4 multicast address.
- **interface** *interface-id*—The interface ID. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No port is configured as a member of a multicast group.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

You cannot register an entry without specifying an interface.

Using the **no** command without a port list removes the entry.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 static 192.168.1.100 interface
fa11
switchxxxxxx(config)# ip igmp snooping vlan 1 static 192.168.1.110 interface
gi1
switchxxxxxx(config)# ip igmp snooping vlan 1 static 192.168.1.200 interface
po1
```

ip igmp snooping vlan mrouter

To register a Layer 2 port as a member of a static multicast group to the bridge table, use the **ip igmp snooping vlan mrouter** Global Configuration mode command.

To remove the ports as the members of a static Mrouter port, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **mrouter interfaces** *interface-id*

no ip igmp snooping vlan *VLAN-LIST* **mrouter interfaces** *interface-id*

Parameter

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- **interfaces** *interface-id*—An interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No port is configured as a member of a static Mrouter port.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no** command without a port list removes the entry.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter interfaces gi1
```

ip igmp snooping vlan forward-all

To enable the IGMP Snooping forward-all static port processing on a VLAN, use the **ip igmp snooping vlan forward-all** Global Configuration mode command.

To disable this feature, use the **no** form of this command.

Syntax

ip igmp snooping vlan *VLAN-LIST* **forward-all interfaces** *interface-id*

no ip igmp snooping vlan *VLAN-LIST* **forward-all interfaces** *interface-id*

Parameter

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forward-all interfaces fa11
switchxxxxxx(config)# ip igmp snooping vlan 1 forward-all interfaces gi1
switchxxxxxx(config)# ip igmp snooping vlan 1 forward-all interfaces po1
```

profile range

To create an IGMP profile, use the **profile range** IGMP-profile Configuration mode command.

Syntax

profile range ip *ip-range* **action** {**permit** | **deny**}

Parameters

- **ip** *ip-range*—Specifies a range of IPv4 addresses. This can be a single IPv4 address or a range of addresses. When entering a range, enter the low IPv4 multicast address, a space, and the high IPv4 multicast address.
- **action permit**—Permits the matching addresses.
- **action deny**—Denies the matching addresses.

Default Configuration

N/A

Command Mode

IGMP-profile Configuration mode

Example

```
switchxxxxxx(config)# ip igmp profile 20
switchxxxxxx(config-igmp-profile)# profile range ip 225.0.0.0 225.0.0.255
action permit
```

show ip igmp filter

To display IGMP profiles for all interfaces or a specific interface, use the **show ip igmp filter** Privileged EXEC mode command.

Syntax

show ip igmp filter [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id* —(Optional) Specifies an interface ID or a list of interface IDs.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp filter
Port ID   |  Profile ID
---------+--------------
     fa1 : 1
     fa2 : 1
     fa3 : 2
     fa4 : 2
     fa5 : None
     fa6 : None
     fa7 : None
     fa8 : None
     fa9 : None
    fa10 : None
    fa11 : None
    fa12 : None
    fa13 : None
    fa14 : None
    fa15 : None
    fa16 : None
```

```
fa17 : None
fa18 : None
fa19 : None
fa20 : None
fa21 : None
fa22 : None
fa23 : None
fa24 : None
 gi1 : None
 gi2 : None
 po1 : None
 po2 : None
 po3 : None
 po4 : None
 po5 : None
 po6 : None
 po7 : None
 po8 : None
```

show ip igmp max-group

To display the maximum number of IGMP groups on a specific interface or all interfaces, use the **show ip igmp max-group** Privileged EXEC mode command.

Syntax

show ip igmp max-group [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

If no interface is specified, the information for all interfaces is displayed.

Example

```
switchxxxxxx# show ip igmp max-group interfaces fa5
Port ID  |  Max Group
---------+-------------
     fa5 : 512
```

show ip igmp max-group action

To display the action for a specific interface or for all interfaces when the number of IGMP groups exceeds the maximum group number, use the **show ip igmp max-group action** Privileged EXEC mode command.

Syntax

show ip igmp max-group action [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

If no interface is specified, the information for all interfaces is displayed.

Example

```
switchxxxxxx# show ip igmp max-group action interface fa5
Port ID  |  Max-groups  Action
---------+--------------------
     fa5 : replacy
```

show ip igmp profile

To display information for all IGMP profiles or for a specific IGMP profile, use the **show ip igmp profile** Privileged EXEC mode command.

Syntax

show ip igmp profile [*profile-index*]

Parameters

- *profile-index*—(Optional) IGMP profile index.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp profile
IP igmp profile index: 1
IP igmp profile action: permit
Range low ip: 10.172.11.1
Range high ip: 10.172.11.20
```

show ip igmp snooping

To display the IGMP Snooping status, use the **show ip igmp snooping** Privileged EXEC mode command.

Syntax

show ip igmp snooping

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp snooping


              IGMP Snooping Status
              --------------------

    Snooping                          : Enabled
    Report Suppression                : Enabled
    Operation Version                 : v2
    Forward Method                    : mac
    Unknown Multicast Action          : Flood


              Packet Statistics
    Total RX                           :  79
    Valid RX                           :  42
    Invalid RX                         :  37
    Other RX                           :  0
    Leave RX                           :  0
    Report RX                          :  0
    General Query RX                   :  0
    Specail Group Query RX             :  0
    Specail Group & Source Query RX    :  0
    Leave TX                           :  0
    Report TX                          :  0
    General Query TX                   :  0
    Special Group Query TX             :  0
    Special Group & Source Query TX    :  0
```

show ip igmp snooping forward-all

To display information for IGMP Snooping forward all, use the **show ip igmp snooping forward-all** Privileged EXEC mode command.

Syntax

show ip igmp snooping forward-all [**vlan** *VLAN_LIST*]

Parameters

- **vlan** *VLAN-LIST*—(Optional) Specifies a VLAN ID or a list of VLANs. (Range: 1 to 4094)

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp snooping forward-all

IGMP Snooping VLAN           : 1
IGMP Snooping static port    : None
IGMP Snooping forbidden port : None

IGMP Snooping VLAN           : 104
IGMP Snooping static port    : None
IGMP Snooping forbidden port : None
```

show ip igmp snooping groups

To display multicast groups learned by IGMP Snooping, use the **show ip igmp snooping groups** Privileged EXEC mode command.

Syntax

show ip igmp snooping groups [**counters** | **dynamic** | **static**]

Parameters

- **counters**—(Optional) Displays IPv4 group total entries.
- **dynamic**—(Optional) Displays dynamic groups.
- **static**—(Optional) Displays static groups.

Command Mode

Privileged EXEC mode

User Guidelines

To display all multicast groups learned by IGMP Snooping, use the **show ip igmp snooping groups** command without parameters.

To display a needed subset of all multicast groups learned by IGMP Snooping, use the **show ip igmp snooping groups** command with parameters.

Example

```
switchxxxxxx# show ip igmp snooping groups
VLAN | Group IP Address |  Type  | Life(Sec) | Port
-----+-----------------+-------+-----------+-----------------
    1 |        238.0.0.0  |  Static|     --      | fa1-24,gi1-2,po1-8


Total Number of Entry = 1
```

show ip igmp snooping mrouter

To display information on dynamically, static, or forbidden learned multicast router port for all VLANs or for a specific VLAN, use the **show ip igmp snooping mrouter** Privileged EXEC mode command.

Syntax

show ip igmp snooping mrouter [**dynamic** | **static** | **forbidden**]

Parameters

- **dynamic**—(Optional) Displays dynamic routers.
- **forbidden**—(Optional) Displays forbidden routers.
- **static**—(Optional) Displays static routers.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp snooping mrouter
Dynamic Mrouter Table
 VID   |  Port   | Expiry Time(Sec)
------+--------+-----------------
Total Entry 0
Static Mrouter Table
 VID   | Port Mask
------+-----------------------
Total Entry 0
Forbidden Mrouter Table
 VID   | Port Mask
```

```
------+------------------------
Total Entry 0
```

show ip igmp snooping querier

To display information for the IGMP Snooping querier, use the **show ip igmp snooping querier** Privileged EXEC mode command.

Syntax

show ip igmp snooping querier

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp snooping querier

  VID   |    State     |    Status    |  Version    |  Querier IP
-------+-------------+-------------+------------+--------------------
     1 |  Disabled    | Non-Querier |   No        |    ------
   104 |  Disabled    | Non-Querier |   No        |    ------

Total Entry 2
```

show ip igmp snooping vlan

To display the IGMP Snooping configuration for specific VLANs, use the **show ip igmp snooping vlan** Privileged EXEC mode command.

Syntax

show ip igmp snooping vlan [*VLAN-LIST*]

Parameters

- *VLAN-LIST*—(Optional) A VLAN ID or a range of VLAN IDs. (Range: 1 to 4094)

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip igmp snooping vlan 1
IGMP Snooping is globally enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 2 oper 2
IGMP Snooping query interval: admin 125 sec oper 125 sec
IGMP Snooping query max response : admin 10 sec oper 10 sec
IGMP Snooping last member query counter: admin 2  oper 2
IGMP Snooping last member query interval: admin 1 sec  oper 1 sec
IGMP Snooping immediate leave: disabled
IGMP Snooping automatic learning of mrouter ports: enabled
```

14

IP Addressing Commands

clear arp-cache

To delete all dynamic IP entries or a specific IP entry from the ARP cache, use the **clear arp-cache** Privileged EXEC mode command.

Syntax

clear arp-cache [*ip-address*]

Parameters

- *ip-address*—(Optional) The IP address to be deleted.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear arp-cache
```

ip default-gateway

To define a default gateway, use the **ip default-gateway** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip default-gateway *IPv4-ADDR*

no ip default-gateway

Parameters

- *IPv4-ADDR*—IPv4 address of the default gateway.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip default-gateway 192.168.1.100
```

ip domain lookup

To enable the IP Domain Naming System (DNS)-based host-name-to-address translation, use the **ip domain lookup** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip domain lookup

no ip domain lookup

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the switch to query domain name for DNS server.

Example

```
switchxxxxxx(config)# ip domain loopkup
```

ip domain name

To define a default domain name that the switch uses to complete unqualified host names, use the **ip domain name** Global Configuration mode command.

To delete the static-defined default domain name, use the **no** form of this command.

Syntax

ip domain name *hostname*

no ip domain name

Parameters

- *hostname*—Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. Length: 1 to 255 characters. Maximum label length of each domain level is 63 characters.

Default Configuration

No default domain name is defined.

Command Mode

Global Configuration mode

User Guidelines

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and the default domain name appended to it before being added to the host table.

Domain names and hostnames are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of each domain level is 63 characters. The maximum name size is 255 bytes.

Example

```
switchxxxxxx(config)# ip domain name website.com
```

ip host

To define the static host-name-to-address mapping in the DNS hostname cache, use the **ip host** Global Configuration mode command

To remove the static-host name-to-address, use the **no** form of this command.

Syntax

ip host *hostname address1* [*address2...address8*]

no ip host *hostname address1* [*address2...address8*]

Parameters

- *hostname*—Name of the host. (Length: 1 to 158 characters. Maximum label length of each domain level is 63 characters.)
- *address1*—Associated host IP address (IPv4 or IPv6, if IPv6 stack is supported).
- *address2...address8*—(Optional) Up to seven additional associated IP addresses, delimited by a single space (IPv4 or IPv6, if IPv6 stack is supported).

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

Hostnames are restricted to ASCII letters A through Z (case-insensitive), the digit 0 through 9, the underscore and the hyphen symbols. A period (.) is used to separate labels.

An IP application will receive the IP addresses in the following order:

- IPv6 addresses in the order specified by the command.
- IPv4 addresses in the order specified by the command.

Use the **no** format of the command with the *address1...address8* argument to delete the specified addresses. The entry is deleted if all its addresses are deleted.

Example

```
switchxxxxxx(config)# ip host accounting.website.com 176.10.23.1
```

ip name-server

To configure the DNS servers, use the **ip name-server** Global Configuration mode command.

To disable the DNS servers, use the **no** form of this command.

Syntax

ip name-server *server-address1* [*server-address2...server-address8*]

no ip name-server

Parameters

- *server-address1*—IPv4 or IPv6 addresses of a single name server.
- *server-address2...server-address8*—(Optional) IPv4 or IPv6 addresses of additional name servers.

Default Configuration

No DNS server is configured.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip name-server 192.168.1.20
switchxxxxxx(config)# ip name-server 192.168.1.20 192.168.1.50
```

management vlan ip-address

To define the IP address for the management VLAN, use the **management vlan ip-address** Global Configuration mode command.

Syntax

management vlan ip-address *ip-address* **mask** *mask*

Parameters

- *ip-address*—The IP address.
- *mask*—The network mask of the IP address.

Default Configuration

The default IP address of the management VLAN is 192.168.1.254.

Command Mode

Global Configuration mode

User Guidelines

If a dynamic IP address is already defined, the user must enter the **no management ip dhcp client** command to disable it before setting a static IP address.

If you modify the static IP address, enter the **no management ip dhcp client** command to automatically add.

Example

The following example configures the management VLAN with IP address 131.108.1.27 and subnet mask 255.255.255.0:

```
switchxxxxxx(config)# management vlan ip address 131.108.1.27 mask
255.255.255.0
```

management vlan ip dhcp client

To acquire an IP address for the management VLAN from the DHCP server, use the **management vlan ip dhcp client** Global Configuration mode command.

To release an acquired IP address, use the **no** form of this command.

Syntax

management vlan ip dhcp client

no management vlan ip dhcp client

Parameters

N/A

Default Configuration

DHCP client is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables the switch to dynamically learn its IP address by using the DHCP protocol.

DHCP client configuration on the switch implicitly removes the static IP address configuration on the management VLAN.

If the switch 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.

The **no management vlan ip dhcp client** command releases any IP address that was acquired, and sends a DHCPRELEASE message.

Example

```
switchxxxxxx(config)# management vlan ip dhcp client
```

show arp

To display all entries in the ARP table, use the **show arp** Privileged EXEC mode command.

Syntax

show arp

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show arp
Address                 HWtype  HWaddress           Flags Mask            Iface
192.168.1.22             ether   00:10:60:DB:6E:FE   C                     eth0
```

show hosts

To display the DNS servers defined on the switch, use the **show hosts** Privileged EXEC mode command.

Syntax

show hosts

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show hosts
```

```
Name/address lookup is enabled


Default Domain Table

                  Domain                          Source   Preference
---------------------------------------------- --------- ----------


Name Server Table

               IP Address                         Source   Preference
---------------------------------------------- --------- ----------


Cache Table
Flags: (STA, OK)
STA - Static
OK - Okay

          Host                  IP Address            Type     State
------------------------ ------------------------ --------- --------
```

show ip

To display the IP address of the management VLAN, use the **show ip** Privileged EXEC mode command.

Syntax

show ip

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip
```

```
IP Address: 192.168.1.254
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

show ip dhcp

To display the IP DHCP status, use the **show ip dhcp** Privileged EXEC mode command.

Syntax

show ip dhcp

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp
DHCP Status : disabled
```

15

IP ARP Inspection Commands

clear ip arp inspection statistics vlan

To clear the Address Resolution Protocol (ARP) Inspection statistics for specific VLANs, use the **clear ip arp inspection statistics vlan** Privileged EXEC mode command.

Syntax

clear ip arp inspection statistics vlan *VLAN-LIST*

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip arp inspection statistics vlan 1
```

ip arp inspection

To enable dynamic ARP inspection on the switch, use the **ip arp inspection** Global Configuration mode command.

To disable dynamic ARP inspection on the switch, use the **no** form of this command.

Syntax

ip arp inspection

no ip arp inspection

Parameters

N/A

Default Configuration

No specific dynamic ARP inspection is performed.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip arp inspection
```

ip arp inspection limit rate

To limit the rate of incoming ARP requests and responses on an interface, use the **ip arp inspection limit rate** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip arp inspection limit rate *VALUE*

no ip arp inspection limit rate

Parameters

- *VALUE*—Maximum number of incoming packets per second that are allowed on the interface. (Range: 1 to 300 pps)

Default Configuration

The default rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.

The rate is unlimited on all trusted interfaces.

The burst interval is 1 second.

Command Mode

Interface Configuration mode

User Guidelines

This command prevents dynamic ARP inspection from using all of the switch resources if a DoS attack occurs.

The rate applies to both trusted and untrusted interfaces. Configure appropriate rates on trunks to process packets across multiple VLANs that enabled the dynamic ARP inspection function.

After the switch receives more than the configured rate of packets every second consecutively over a number of burst seconds, the interface is placed into an error-disabled state.

Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection limit** command, the interface reverts to its default rate limit.

You should configure trunk ports with higher rates to reflect their aggregation. When the rate of incoming packets exceeds the user-configured rate, the switch places the interface into an error-disabled state. The errordisable recovery feature automatically removes the port from the error-disabled state according to the recovery setting.

The rate of incoming ARP packets on EtherChannel ports equals to the sum of the incoming rate of ARP packets from all channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on all channel members.

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# ip arp inspection limit rate 150
```

ip arp inspection trust

To configure the trust state that determines which incoming ARP packets are inspected for an interface, use the **ip arp inspection trust** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip arp inspection trust

no ip arp inspection trust

Parameters

N/A

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration mode

User Guidelines

The switch does not check ARP packets that are received on the trusted interface. It only forwards these packets.

For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination.

Example

```
switchxxxxxx(config)# interface gi9
switchxxxxxx(config-if)# ip arp inspection trust
```

ip arp inspection validate

To validate ARP packets on the switch, use the **ip arp inspection validate** Global Configuration mode command.

To disable validating ARP packets, use the **no** form of this command.

Syntax

ip arp inspection validate {**dst-mac** | **ip** [**allow-zeros**] | **src-mac**}

no ip arp inspection validate {**dst-mac** | **ip** [**allow-zeros**] | **src-mac**}

Parameters

- **dst-mac**—Compares the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, the packets with different MAC addresses are classified as invalid and are dropped.
- **ip**—Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are compared in all ARP requests and responses. Target IP addresses are compared only in ARP responses.
- **allow-zeros**—(Optional) Modifies the IP validation test so that ARPs with an address of 0.0.0.0 are not denied.
- **src-mac**—Compares the source MAC address in the Ethernet header against the sender MAC address in ARP body. This check is performed on both ARP requests and responses. When enabled, the packets with different MAC addresses are classified as invalid and are dropped.

Default Configuration

Validating ARP packets is disabled.

Command Mode

Global Configuration mode

User Guidelines

You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables **src-mac** and **dst-mac** validations, and a second command enables IP validation only, the **src-mac** and **dst-mac** validations are disabled as a result of the second command.

The **allow-zeros** keyword interacts with ARP ACLs in this way:

- If you configure an ARP ACL to deny ARP probes, they are dropped even if the **allow-zeros** keyword is specified.
- If you configure an ARP ACL that specifically permits ARP probes and configure the **ip arp inspection validate ip** command, ARP probes are dropped unless you enter the **allow-zeros** keyword.

Example

```
switchxxxxxx(config)# ip arp inspection validate dst-mac
switchxxxxxx(config)# ip arp inspection validate src-mac
switchxxxxxx(config)# ip arp inspection validate ip
switchxxxxxx(config)# ip arp inspection validate ip allow-zeros
```

ip arp inspection vlan

To enable dynamic ARP inspection on specific VLANs, use the **ip arp inspection vlan** Global Configuration mode command.

To disable dynamic ARP inspection on specific VLANs, use the **no** form of this command.

Syntax

ip arp inspection vlan *VLAN-LIST*

no ip arp inspection vlan *VLAN-LIST*

Parameters

- *VLAN-LIST*—Specifies a VLAN ID or a range of VLAN IDs. (Range: 1 to 4094)

Default Configuration

ARP inspection is disabled on all VLANs.

Command Mode

Global Configuration mode

User Guidelines

You must specify the VLANs on which to enable dynamic ARP inspection. Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

Example

```
switchxxxxxx(config)# ip arp inspection vlan 5
```

show ip arp inspection

To show the ARP Inspection status, use the **show ip arp inspection** Privileged EXEC mode command.

Syntax

show ip arp inspection

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip arp inspection
Dynamic ARP Inspection      : disabled
Source Mac Validation       : disabled
Destination Mac Validation : disabled
IP Address Validation       : disabled
Enable on Vlans              : None
```

The following table describes the significant fields shown in the example:

Field	Description
Dynamic ARP Inspection	Shows whether dynamic ARP Inspection is enabled or disabled on the switch.

Field	Description
Source Mac Validation	Shows whether to compare the source MAC address in the Ethernet header against the sender MAC address in ARP body.
Destination Mac Validation	Shows whether to compare the destination MAC address in the Ethernet header against the target MAC address in ARP body.
IP Address Validation	Shows whether to compare the ARP body for invalid and unexpected IP addresses.
Enable on Vlans	Shows whether dynamic ARP Inspection is enabled or disabled on the VLANs.

show ip arp inspection interfaces

To show the ARP Inspection configuration for specific interfaces, use the **show ip arp inspection interfaces** Privileged EXEC mode command.

Syntax

show ip arp inspection interfaces *interface-id*

Parameters

- *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip arp inspection interfaces gi1
 Interfaces | Trust State |  Rate (pps)
------------+-------------+-------------
gi1          | Untrusted   |   15
```

The following table describes the significant fields shown in the example:

Field	Description
Interfaces	Port or LAG on which ARP Inspection trust mode can be enabled.
Trust State	Shows whether ARP Inspection trust mode is enabled or disabled on the interface. ▪ Enabled—The port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests and replies sent to and from the interface. ▪ Disabled—The port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests and replies sent to and from the interface. This is the default value.
Rate (pps)	Maximum rate that is allowed on the interface.

show ip arp inspection statistics

To show the ARP Inspection statistics for all VLANs or for specific VLANs, use the **show ip arp inspection statistics** Privileged EXEC mode command.

Syntax

show ip arp inspection statistics [**VLAN** *VLAN-LIST*]

Parameters

- *VLAN-LIST*—(Optional) Specifies a VLAN ID or a list of VLAN IDs. (Range: 1 to 4094)

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip arp inspection statistics vlan 1
Vlan| Forward |Source MAC Failures|Dest MAC Failures|SIP Validation
Failures|DIP Validation Failures|IP-MAC Mismatch Failures
```

```
----+---------+------------------+----------------+----------------------
+----------------------+------------------------
 1|        0 |                  0 |              0 |                      0 |
                   0 |           0
```

The following table describes the significant fields shown in the example:

Field	Description
VLAN	VLAN ID.
Forward	Total number of ARP packets forwarded by the VLAN.
Source MAC Failures	Total number of ARP packets that include wrong source MAC addresses.
Dest MAC Failures	Total number of ARP packets that include wrong destination MAC addresses.
SIP Validation Failures	Total number of ARP packets that the source IP address validation fails.
DIP Validation Failures	Total number of ARP packets that the destination IP address validation fails.
IP-MAC Mismatch Failures	Total number of ARP packets that the IP address does not match the MAC address.

16

IP DHCP Snooping Commands

clear ip dhcp snooping binding

To clear the DHCP snooping binding entries for all addresses or for specific IP address, use the **clear ip dhcp snooping binding** Privileged EXEC mode command.

Syntax

clear ip dhcp snooping binding {* | *IPv4-Addr*}

Parameters

- ***—Clears all dynamic entries
- *IPv4-Addr*—The entry for an IPv4 address.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip dhcp snooping binding 192.168.1.1
```

clear ip dhcp snooping binding interface

To clear the DHCP snooping binding entries for specific interfaces, use the **clear ip dhcp snooping binding interface** Privileged EXEC mode command.

Syntax

clear ip dhcp snooping binding interface *interface-id*

Parameters

- *interface-id*—The interface ID, which can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip dhcp snooping binding interface fa5
```

clear ip dhcp snooping binding vlan

To clear the DHCP snooping binding entries for specific VLANs, use the **clear ip dhcp snooping binding vlan** Privileged EXEC mode command.

Syntax

clear ip dhcp snooping binding vlan *vlan-id*

Parameters

- *vlan-id*—The VLAN ID.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip dhcp snooping binding vlan 1
```

clear ip dhcp snooping database statistics

To clear the DHCP snooping database statistics, use the **clear ip dhcp snooping database statistics** Privileged EXEC mode command.

Syntax

clear ip dhcp snooping database statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip dhcp snooping database statistics
```

clear ip dhcp snooping interfaces statistics

To clear the DHCP snooping database statistics for specific interfaces, use the **clear ip dhcp snooping interfaces statistics** Privileged EXEC mode command.

Syntax

clear ip dhcp snooping interfaces *interface-id* **statistics**

Parameters

- *interface-id*—An interface ID or a list of interfaces. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip dhcp snooping interfaces fa5 statistics
```

ip dhcp snooping

To enable DHCP snooping globally on the switch, use the **ip dhcp snooping** Global Configuration mode command.

To disable DHCP snooping globally, use the **no** form of this command.

Syntax

ip dhcp snooping

no ip dhcp snooping

Parameters

N/A

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

To apply any DHCP snooping configuration, you must enable DHCP snooping globally on the switch. DHCP snooping is not active until you enable DHCP snooping on a VLAN by using the **ip dhcp snooping vlan** Global Configuration mode command.

Example

```
switchxxxxxx(config)# ip dhcp snooping
```

ip dhcp snooping database

To configure the DHCP snooping binding database agent, use the **ip dhcp snooping database** Global Configuration mode command.

To disable the agent, reset the timeout value, or reset the write-delay value, use the **no** form of this command.

Syntax

ip dhcp snooping database {**flash** | **tftp** {*IPv4-ADDR NAME* | *HOSTNAME NAME*} | **timeout** *VALUE* | **write-delay** *VALUE*}

no ip dhcp snooping database [**timeout** | **write-delay**]

Parameters

- **flash**—Specifies that the database agent is in the flash memory.
- **tftp** *IPv4-ADDR NAME*—Specifies the IP address of the remote TFTP server and the file name of the backup file.
- **tftp** *HOSTNAME NAME*—Specifies the hostname of the remote TFTP server and the file name of the backup file.
- **timeout** *VALUE*—Specifies the timeout in seconds when to stop the database transfer process after the DHCP snooping binding database changes. (Range: 0 to 86400 seconds. Use 0 to define an infinite duration.)
- **write-delay** *VALUE*—Specifies the duration in seconds for which the transfer should be delayed after the binding database changes. (Range: 15 to 86400 seconds)

Default Configuration

The URL for the database agent is not defined.

The default timeout is 300 seconds (5 minutes).

The default write-delay is 300 seconds (5 minutes).

Command Mode

Global Configuration mode

User Guidelines

The DHCP snooping binding database can have up to 256 bindings. Because both NVRAM and flash memory have limited storage capacity, we recommend that you store a binding file on a TFTP server. You must create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write bindings to the binding file at that URL for the first time.

To save the DHCP snooping binding database in the switch NVRAM, use the **ip dhcp snooping database flash** command.

To disable the agent, use the **no ip dhcp snooping database** command.

To reset the timeout value, use the **no ip dhcp snooping database timeout** command.

To reset the write-delay value, use the **no ip dhcp snooping database write-delay** command.

Example

```
switchxxxxxx(config)# ip dhcp snooping database flash
switchxxxxxx(config)# ip dhcp snooping database tftp 192.168.1.20 test1
switchxxxxxx(config)# ip dhcp snooping database tftp test-host test2
switchxxxxxx(config)# ip dhcp snooping database timeout 1200
switchxxxxxx(config)# ip dhcp snooping database write-delay 3000
```

ip dhcp snooping information option

To enable DHCP option-82 data insertion, use the **ip dhcp snooping information option** Global Configuration mode command.

To disable DHCP option-82 data insertion, use the **no** form of this command.

Syntax

ip dhcp snooping information option [**format remote-id** *STRING*]

no ip dhcp snooping information option [**format remote-id**]

Parameters

- **format remote-id** *STRING*—(Optional) Enables the remote ID string. (String length: 1 to 63 characters)

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

You must enable DHCP snooping globally by using the **ip dhcp snooping** Global Configuration mode command to apply any DHCP snooping configuration.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. The DHCP server then echoes the option-82 field in the DHCP reply.

The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When both the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sends the DHCP request.

Example

```
switchxxxxxx(config)# ip dhcp snooping information option
switchxxxxxx(config)# ip dhcp snooping information option format remote-id
test
```

ip dhcp snooping information option allow-untrusted

To configure an aggregation switch to accept DHCP packets with option-82 information which are received on the untrusted ports that might be connected to an edge switch, use the **ip dhcp snooping information option allow-untrusted** Interface Configuration mode command.

To configure the switch to drop these packets from the edge switch, use the **no** form of this command.

Syntax

ip dhcp snooping information option allow-untrusted [replace]

no ip dhcp snooping information option allow-untrusted

Parameters

- **replace—**(Optional) Replaces DHCP packets with option-82 information.

Default Configuration

The switch drops DHCP packets with option-82 information which are received on the untrusted ports that might be connected to an edge switch.

Command Mode

Interface Configuration mode

User Guidelines

You may want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You may also want to enable the DHCP security features, such as DHCP snooping, IP source guard, or dynamic ARP inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information, and you want to use DHCP snooping on an aggregation switch, enter the **ip dhcp snooping information option allow-untrusted** command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable the DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.

Example

```
switchxxxxxx(config)# interface fa3
switchxxxxxx(config-if)# ip dhcp snooping information option allow-untrusted
```

ip dhcp snooping limit rate

To configure the number of DHCP messages that an interface can receive per second, use the **ip dhcp snooping limit rate** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip dhcp snooping limit rate *VALUE*

no ip dhcp snooping limit rate

Parameters

- *VALUE*—Number of DHCP messages that an interface can receive per second.

Default Configuration

DHCP snooping rate limiting is disabled.

Command Mode

Interface Configuration mode

User Guidelines

The rate limit normally applies to untrusted interfaces. If you want to configure rate limiting for trusted interfaces, trusted interfaces may aggregate DHCP traffic on multiple VLANs (some of which may not be snooped) on the switch, and you will need to adjust the interface rate limit to a higher value.

If the rate limit is exceeded, the interface is error-disabled. If you enable error recovery by entering the **errdisable recovery cause dhcp-rate-limit** Global Configuration mode command, the interface retries the operation again when all causes have timed out. If the error recovery function is not enabled, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** Interface Configuration mode commands.

Example

```
switchxxxxxx(config)# interface fa7
switchxxxxxx(config-if)# ip dhcp snooping limit rate 100
```

ip dhcp snooping trust

To configure a port as trusted for DHCP snooping purposes, use the **ip dhcp snooping trust** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Parameters

N/A

Default Configuration

DHCP snooping trust is disabled.

Command Mode

Interface Configuration mode

User Guidelines

Configure the ports that are connected to a DHCP server or to other switches or routers as trusted ports. Configure the ports that are connected to DHCP clients as untrusted ports.

Example

```
switchxxxxxx(config)# interface fa3
switchxxxxxx(config-if)# ip dhcp snooping trust
```

ip dhcp snooping verify mac-address

To configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address, use the **ip dhcp snooping verify mac-address** Global Configuration mode command.

To configure the switch to not verify the MAC addresses, use the **no** form of this command.

Syntax

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies whether the source MAC address and the DHCP client hardware address can match or not. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

Example

```
switchxxxxxx(config)# ip dhcp snooping verify mac-address
```

ip dhcp snooping vlan

To enable DHCP snooping on specific VLANs, use the **ip dhcp snooping vlan** Global Configuration mode command.

To disable DHCP snooping on specific VLANs, use the **no** form of this command.

Syntax

ip dhcp snooping vlan *VLAN-LIST*

no ip dhcp snooping vlan *VLAN-LIST*

Parameters

- *VLAN-LIST*—A VLAN ID or a range of VLAN IDs.

Default Configuration

DHCP snooping is disabled on all VLANs.

Command Mode

Global Configuration mode

User Guidelines

You must first globally enable DHCP snooping on the switch before enabling DHCP snooping on a VLAN.

Example

```
switchxxxxxx(config)# ip dhcp snooping vlan 7
```

ip dhcp snooping vlan information option circuit-id

To configure the option-82 circuit-ID suboption, use the **ip dhcp snooping vlan information option circuit-id** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip dhcp snooping vlan *VLAN-LIST* **information option circuit-id** *STRING*

no ip dhcp snooping vlan *VLAN-LIST* **information option circuit-id**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs. (Range:1 to 4094)
- *STRING*—A circuit ID, using from 1 to 64 ASCII characters (no spaces).

Default Configuration

N/A

Command Mode

Interface Configuration mode

User Guidelines

You must globally enable DHCP snoopingDHCP snooping on the switch by using the **ip dhcp snooping** Global Configuration mode command to apply any DHCP snooping configuration.

When the option-82 feature is enabled, the default circuit-ID suboption is the switch VLAN and port identifier in the format of **vlan-mod-port**. This command allows you to configure a string of ASCII characters to be the circuit ID. When you want to override the **vlan-mod-port** format type and use the circuit ID to define the subscriber information, use the **override** keyword.

Example

```
switchxxxxxx(config)# interface fa7
switchxxxxxx(config-if)# ip dhcp snooping vlan 3 information option circuit-id test
```

renew ip dhcp snooping database

To renew the DHCP snooping binding database, use the **renew ip dhcp snooping database** Privileged EXEC command.

Syntax

renew ip dhcp snooping database

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# renew ip dhcp snooping database
```

show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** Privileged EXEC command.

Syntax

show ip dhcp snooping

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp snooping

DHCP Snooping             : enabled
Enable on following Vlans : None
Verification of hwaddr    : disabled
Insertion of option 82    : disabled
    circuit-id default format: vlan-port
    remote-id:               : vlan1_md_fa11
```

show ip dhcp snooping binding

To display the DHCP snooping binding configuration for all interfaces, use the **show ip dhcp snooping binding** Privileged EXEC mode command.

Syntax

show ip dhcp snooping binding

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp snooping binding

Bind Table: Maximum Binding Entry Number 191
  Port   | VID  |    MAC Address    |       IP        |    Type     | Lease Time
--------+------+-------------------+-----------------+-------------+--------
---

Total Entry: 0
```

show ip dhcp snooping database

To display the status of the DHCP snooping binding database agent, use the **show ip dhcp snooping database** Privileged EXEC mode command.

Syntax

show ip dhcp snooping database

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp snooping database

Type : None
FileName :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : None
Delay Timer Expiry : Not Running
Abort Timer Expiry :Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     0
```

```
Successful Transfers :      0   Failed Transfers :      0
Successful Reads     :      0   Failed Reads     :      0
Successful Writes    :      0   Failed Writes    :      0
```

show ip dhcp snooping information option format remote-id

To display the DHCP snooping option 82 format remote ID, use the **show ip dhcp snooping information option format remote-id** Privileged EXEC mode command.

Syntax

show ip dhcp snooping information option format remote-id

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp snooping information option format remote-id
Remote ID: vlan-md-fa11
```

show ip dhcp snooping interfaces

To display the DHCP snooping configuration for specific interfaces, use the **show ip dhcp snooping interfaces** Privileged EXEC mode command.

Syntax

show ip dhcp snooping interfaces *interface-id*

Parameters

- *interface-id*—An interface ID or a list of interfaces. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp snooping interfaces fa1-5
 Interfaces | Trust State |  Rate (pps)
----------+-------------+-------------
 fa1        | Untrusted   | None
 fa2        | Untrusted   | None
 fa3        | Untrusted   | None
 fa4        | Untrusted   | None
 fa5        | Trusted      | 50
```

show ip dhcp snooping interfaces statistics

To display the DHCP snooping statistics for specific interfaces, use the **show ip dhcp snooping interfaces statistics** Privileged EXEC mode command.

Syntax

show ip dhcp snooping interfaces *interface-id* **statistics**

Parameters

- *interface-id*—An interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip dhcp snooping interfaces fa1-5 statistics
 Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped |
Untrust Port With Option82 Dropped | Invalid Drop
-----------+-----------+----------------------+----------------------+------
------------------------------+--------------
 fa1        | 0         | 0                    | 0                    | 0
                            | 0
 fa2        | 0         | 0                    | 0                    | 0
                            | 0
 fa3        | 0         | 0                    | 0                    | 0
```

```
                                    | 0
fa4          | 0          | 0                    | 0                    | 0
                                    | 0
fa5          | 0          | 0                    | 0                    | 0
                                    | 0
```

17

IP Source Guard Commands

ip source binding

To add a static IP source binding rule for all interfaces or for an interface, use the **ip source binding** Global Configuration mode command.

To delete a static IP source binding rule for all interfaces or for an interface, use the **no** form of this command.

Syntax

ip source binding *MAC-Addr* **vlan** *VLAN-LIST IPv4-Addr* **interface** *interface-id*

no ip source binding *MAC-Addr* **vlan** *VLAN-LIST IPv4-Addr* **interface** *interface-id*

Parameters

- *MAC-Addr*—MAC address for IP source binding.
- **vlan** *VLAN-LIST*—Specifies a VLAN ID or a range of VLAN IDs for IP source binding.
- *IPv4-Addr*—IP address for IP source binding.
- **interface** *interface-id*—Specifies an interface ID or a list of interfaces. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No IP source binding rule is configured.

Command Mode

Global Configuration mode

User Guidelines

A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number. The entry is based on the MAC address and the VLAN number. If you modify an entry by changing only the IP address, the switch updates the entry instead of creating a new one.

Example

```
switchxxxxxx(config)# ip source binding 00:aa:bb:cc:dd:ee vlan 7 192.168.1.50
interface fa1
switchxxxxxx(config)# ip source binding 00:bb:bb:cc:dd:ee vlan 7 192.168.1.60
interface gi1
switchxxxxxx(config)# ip source binding 00:cc:bb:cc:dd:ee vlan 10
192.168.1.90 interface po1
```

ip source binding max-entry

To set the maximum number of IP source binding rules on an interface, use the **ip source binding max-entry** Interface Configuration mode command.

Syntax

ip source binding max-entry {*value* | **no-limit**}

Parameters

- *value*—The maximum number of binding entries. (Range: 1 to 50)
- **no-limit**—Specifies no limit for this rule.

Default Configuration

The default is no limit.

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi13
switchxxxxxx(config-if)# ip source binding max-entry 20
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** Interface Configuration mode command.

To disable IP source guard on an interface, use the **no** form of this command.

Syntax

ip verify source [**mac-and-ip**]

no ip verify source

Parameters

- **mac-and-ip**—(Optional) Enables IP source guard with IP and MAC address filtering. If you do not enter the **mac-and-ip** keyword, IP address filtering is enabled by default.

Default Configuration

IP source guard is disabled.

Command Mode

Interface Configuration mode

User Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** Interface Configuration mode command.

To enable IP source guard with source IP and MAC address filtering, use the **ip verify source mac-and-ip** Interface Configuration mode command.

Example

```
switchxxxxxx(config)# interface gi13
switchxxxxxx(config-if)# ip verify source mac-and-ip
```

show ip source binding

To show information for all IP source binding rules defined on the switch, use the **show ip source binding** Privileged EXEC mode command.

Syntax

show ip source binding [**dynamic** | **static**]

Parameters

- **dynamic**—(Optional) Displays information for IP source bindings that were learned by DHCP snooping.
- **static**—(Optional) Displays information for static IP source bindings.

Command Mode

Privileged EXEC mode

User Guidelines

The **show ip source binding** command output shows all dynamic and static IP source binding entries in the binding database.

Example

```
switchxxxxxx# show ip source binding

Bind Table: Maximum Binding Entry Number 191
  Port  | VID  |    MAC Address    |       IP        |    Type     | Lease Time
--------+------+-------------------+-----------------+-------------+--------
   fa11 |    2 | 00:03:6D:01:10:A0 |   192.168.1.77(255.255.255.255)|
Static    | NA

Total Entry: 1
```

The following table describes the significant fields shown in the example:

Field	Description
Port	Interface number.
VID	Identifier of the VLAN with which the address is associated.

Field	Description
MAC Address	MAC address of the interface.
IP	IP address of the interface.
Type	IP address type. The possible field values are: ▪ Dynamic—Indicates that the IP address is dynamically created. ▪ Static—Indicates that the IP address is a static IP address.
Lease Time	The amount of time that the IP address is active. IP addresses whose lease times are expired are deleted from the database.

show ip verify source interfaces

To show the IP source guard configuration for specific interfaces, use the **show ip verify source interfaces** Privileged EXEC mode command.

Syntax

show ip verify source interfaces [*interface-id*]

Parameters

- *interface-id*—(Optional) An interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip verify source interfaces fa1-10
  Port   |     Status     | Max Entry | Current Entry
---------+----------------+-----------+---------------
    fa1  |       disabled | No Limit  |   1
    fa2  |       disabled | No Limit  |   0
    fa3  |       disabled | No Limit  |   0
    fa4  |       disabled | No Limit  |   0
    fa5  |       disabled | No Limit  |   0
```

```
 fa6 |       disabled | No Limit  |   0
 fa7 |       disabled | No Limit  |   0
 fa8 |       disabled | No Limit  |   0
 fa9 |       disabled | No Limit  |   0
fa10 |       disabled | No Limit  |   0
```

The following table describes the significant fields shown in the example:

Field	Description
Port	Interface number.
Status	Shows whether IP source guard is enabled or disabled on the interface.
Max Entry	Maximum number of binding entries allowed in the IP source binding database.
Current Entry	Current number of binding entries in the IP source binding database.

18

IPv6 Addressing Commands

ipv6 default-gateway

To define an IPv6 default gateway, use the **ipv6 default-gateway** Global Configuration mode command.

Syntax

ipv6 default-gateway *ipv6-address*

Parameters

- *ipv6-address*—The IPv6 address of the next hop that can be used to reach the required network.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

Configuring a new default gateway without deleting the previous configured information overwrites the previous configuration.

A configured default gateway has a higher precedence over an automatically advertised by using a router advertisement message.

Precedence takes effect after the configured default gateway is reachable.

Reachability state is not verified automatically by the neighbor discovery protocol. Router reachability can be confirmed by either receiving a Router Advertisement message or containing the router's MAC address. Another option to force the reachability confirmation is to ping the router link-local address (this will initiate the neighbor discovery process).

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Example

```
switchxxxxxx(config)# ipv6 default-gateway fe80::abcd
```

management vlan ipv6-address

To configure an IPv6 address for the management VLAN, use the **management vlan ipv6-address** Global Configuration mode command.

Syntax

management vlan ipv6-address *ipv6-address* **prefix-length** *prefix-length*

Parameters

- *ipv6-address*—The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
- **prefix-length** *prefix-length*—Specifies the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). (Range: 0 to 128)

Default Configuration

No IPv6 address is defined for the management VLAN.

Command Mode

Global Configuration mode

User Guidelines

If the value specified for the prefix-length argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Example

```
switchxxxxxx(config)# management vlan ipv6-address 3000::123 prefix-length
64
```

management vlan ipv6-address-autoconfig

To enable IPv6 address autoconfiguration on the switch, use the **management vlan ipv6-address-autoconfig** Global Configuration mode command. Addresses are configured depending on the prefixes received in the Router Advertisement messages.

To disable IPv6 address autoconfiguration on the switch, use the **no** form of this command.

Syntax

management vlan ipv6-address-autoconfig

no management vlan ipv6-address-autoconfig

Parameters

N/A

Default Configuration

IPv6 address autoconfiguration is enabled on the switch. No IPv6 address is assigned by default.

Command Mode

Global Configuration mode

User Guidelines

When IPv6 address autoconfiguration is enabled, the router solicitation ND procedure is initiated to discover a router and assign IP addresses to the switch, based on the advertised on-link prefixes.

When disabling IPv6 address autoconfiguration, automatically generated addresses that were assigned to the switch are removed.

The default state of IPv6 address autoconfiguration is enabled.

Example

```
switchxxxxxx(config)# management vlan ipv6-address-autoconfig
```

management vlan ipv6-address-dhcp

To acquire an IPv6 address on an interface from the DHCPv6 server, use the **management vlan ipv6-address-dhcp** Global Configuration mode command.

To remove the IPv6 address from the interface, use the **no** form of this command.

Syntax

management vlan ipv6-address-dhcp

no management vlan ipv6-address-dhcp

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

The **management vlan ipv6-address-dhcp** Global Configuration command allows the switch to dynamically learn its IPv6 address by using DHCP.

Example

```
switchxxxxxx(config)# management vlan ipv6-address-dhcp
```

show ipv6

To display the IPv6 configuration of the switch, use the **show ipv6** Privileged EXEC mode command.

Syntax

show ipv6

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6
IPv6 DHCP Configuration     : Disabled
IPv6 DHCP DUID              :
IPv6 Auto Configuration     : Enabled
IPv6 Link Local Address     : fe80::2e36:f8ff:fe4b:e227/64
IPv6 static Address         : ::/0
IPv6 static Gateway Address : ::
IPv6 in use Address         : fe80::2e36:f8ff:fe4b:e227/64
```

show ipv6 dhcp

To display the IPv6 DHCP parameters configured on the switch, use the **show ipv6 dhcp** Privileged EXEC mode command.

Syntax

show ipv6 dhcp

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx(config)# show ipv6 dhcp
DHCPv6 Status : enabled
```

19

IPv6 MLD Snooping Commands

clear ipv6 mld snooping groups

To delete the IPv6 multicast Listener Discovery (MLD) group cache entries, use the **clear ipv6 mld snooping groups** Privileged EXEC mode command.

Syntax

clear ipv6 mld snooping groups [**dynamic** | **static**]

Parameters

- **dynamic**—(Optional) Deletes dynamic MLD groups.
- **static**—(Optional) Deletes static MLD groups.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ipv6 mld snooping groups
```

clear ipv6 mld snooping statistics

To clear the IPv6 MLD snooping statistics, use the **clear ipv6 mld snooping statistics** Privileged EXEC mode command.

Syntax

clear ipv6 mld snooping statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ipv6 mld snooping statistics
```

ipv6 mld filter

To control whether or not all hosts on a Layer 2 interface can join one or more IPv6 multicast groups by applying a MLD profile to the interface, use the **ipv6 mld filter** Interface Configuration mode command.

To remove a MLD profile from the interface, use the **no** form of this command.

Syntax

ipv6 mld filter *profile-number*

no ipv6 mld filter

Parameter

- *profile-number*—The MLD profile number to be applied. (Range: 1 to 128)

Default Configuration

No MLD profiles are applied.

Command Mode

Interface Configuration mode

User Guidelines

You can apply the MLD profiles only to Layer 2 physical or EtherChannel interfaces.

A MLD profile can be applied to one or more switch interfaces, but one interface can have only one profile applied to it.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ipv6 mld filter 22
```

ipv6 mld max-groups

To set the maximum number of MLD groups that an interface can join or to configure the MLD throttling action when the maximum number of entries in the forwarding table is reached, use the **ipv6 mld max-groups** Interface Configuration mode command.

To set the maximum back to the default setting, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

Syntax

ipv6 mld max-groups *number*

no ipv6 mld max-groups *number*

ipv6 mld max-groups action {**deny** | **replace**}

Parameters

- *number*—The maximum number of MLD groups that an interface can join.
- **action deny**—When the maximum number of entries in the MLD snooping forwarding table is reached, drops the next MLD join report. This is the default action.
- **action replace**—When the maximum number of entries in the MLD snooping forwarding table is reached, replaces the existing group with the new group for which the MLD report was received.

Command Mode

Interface Configuration mode

User Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces.

Follow these guidelines when configuring the MLD throttling action:

- If you configure the throttling action as deny and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries in the forwarding table is reached, the switch drops the next MLD report received on the interface.
- If you configure the throttling action as replace and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries in the forwarding table is reached, the switch replaces a randomly selected multicast entry with the received MLD report.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ipv6 mld max-groups 25
switchxxxxxx(config-if)# ipv6 mld max-groups action replace
```

ipv6 mld profile

To create a MLD profile and enter the MLD Profile Configuration mode, use the **ipv6 mld profile** Global Configuration mode command. From this mode, you can specify the configuration of the IGMP profile to be used for filtering MLD membership reports from a switch port.

To delete a MLD profile, use the **no** form of this command.

Syntax

ipv6 mld profile *profile-number*

no ip igmp profile *profile-number*

Parameters

- *profile-number*—The MLD profile number. (Range:1 to 128)

Default Configuration

No IGMP profiles are defined.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ipv6 mld profile 20
switchxxxxxx(config-mld-profile)#
```

ipv6 mld snooping

To enable IPv6 MLD snooping on the switch, use the **ipv6 mld snooping** Global Configuration mode command.

To disable IPv6 MLD snooping, use the **no** form of this command.

Syntax

ipv6 mld snooping [**version** {**1** | **2**}]

no ipv6 mld snooping

Parameters

- **version 1**—(Optional) Specifies the MLD operation version as v1.
- **version 2**—(Optional) Specifies the MLD operation version as v2.

Default Configuration

The default MLD version is v1.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ipv6 mld snooping
```

ipv6 mld snooping report-suppression

To enable IPv6 MLD snooping report suppression on the switch, use the **ipv6 mld snooping report-suppression** Global Configuration mode command.

To disable this feature, use the **no** form of this command.

Syntax

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Parameters

N/A

Default Configuration

IPv6 MLD snooping report suppression is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

MLD snooping listener message suppression is equivalent to IGMP Snooping report suppression. When enabling MLD snooping report suppression, received MLDv1 reports to a group are forwarded to IPv6 multicast routers only once in every report-forward time. This function prevents the forwarding of duplicate reports.

Example

```
switchxxxxxx(config)# ipv6 mld snooping report-suppression
```

ipv6 mld snooping vlan

To configure the IPv6 MLD snooping parameters on the VLANs, use the **ipv6 mld snooping vlan** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST*

no ipv6 mld snooping vlan *VLAN-LIST*

Parameters

- *VLAN-LIST*—A VLAN ID or a range of VLAN IDs. (Range: 1 to 4094)

Default Configuration

MLD snooping is disabled on all VLANs.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 100
```

ipv6 mld snooping vlan immediate-leave

To enable MLD snooping immediate leave processing on the VLANs, use the **ipv6 mld snooping vlan immediate-leave** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **immediate-leave**

no ipv6 mld snooping vlan *VLAN-LIST* **immediate-leave**

Parameters

- *VLAN-LIST*—A VLAN ID or a range of VLAN IDs on which both MLD snooping and immediate leave are enabled.

Default Configuration

MLD immediate leave processing is disabled.

Command Mode

Global Configuration mode

User Guidelines

You should configure the immediate leave feature only when there is a maximum of one receiver on each interface in the VLAN.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 3 fastleave
```

ipv6 mld snooping vlan forbidden mrouter

To forbid a port from being defined as a multicast router port by static configuration or by automatic learning, use the **ipv6 mld snooping vlan forbidden mrouter** Global Configuration mode command.

To revert to its default settings, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **forbidden mrouter interfaces** *interface-id*

no ipv6 mld snooping vlan *VLAN-LIST* **forbidden mrouter interfaces** *interface-id*

Parameters

- *VLAN-LIST*—A VLAN ID or a range of VLAN IDs.
- **interfaces** *interface-id*—Specifies an interface or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No ports are defined.

Command Mode

Global Configuration mode

User Guidelines

A port that is a forbidden-mrouter-port cannot be a multicast router port (for example, cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter interfaces gi1
```

ipv6 mld snooping vlan forbidden forward-all

To enable the MLD snooping forbidden forward-all processing on the VLANs, use the **ipv6 mld snooping vlan forbidden-port** Global Configuration mode command.

To disable this feature, use the **no** form of this command.

Syntax

ip6 mld snooping vlan *VLAN-LIST* **forbidden forward-all interfaces** *interface-id*

no ip6 mld snooping vlan *VLAN-LIST* **forbidden forward-all interfaces** *interface-id*

Parameters

- *VLAN-LIST*—A VLAN ID or a range of VLAN IDs.
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No port is configured as a member of a multicast group.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden forward-all
interfaces fa1
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden forward-all
interfaces gi1
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden forward-all
interfaces po5
```

ipv6 mld snooping vlan last-member-query-count

To configure IPv6 MLD multicast Address Specific Queries (MASQs) that will be sent before aging out a client, use the **ipv6 mld vlan snooping last-member-query-count** Global Configuration mode command.

To revert to the default settings, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **last-member-query-count** *VALUE*

no ipv6 mld snooping vlan *VLAN-LIST* **last-member-query-count**

Parameters

- *VLAN-LIST*—A VLAN ID or a range of VLAN IDs.
- *VALUE*—The number of last member queries. (Range: 1 to 7)

Default Configuration

The default last member query count is 2.

Command Mode

Global Configuration mode

User Guidelines

In MLD snooping, the IPv6 multicast router periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (which it should not be if multiple clients for a group exist on the same port), the configured last-listener query count determines the number of MASQs that are sent before a MLD client is aged out.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 2 last-member-query-count 5
```

ipv6 mld snooping vlan last-member-query-interval

To configure IPv6 MLD snooping last-listener query interval on the switch or on a VLAN, use the **ipv6 mld snooping vlan last-member-query-interval** Global Configuration mode command. This time interval is the maximum time that a multicast router waits after issuing an MASQ before deleting a port from the multicast group.

To revert to the default settings, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **last-member-query-interval** *VALUE*

no ipv6 mld snooping vlan *VLAN-LIST* **last-member-query-interval**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- *VALUE*—The MLD query interval in seconds. (Range: 1 to 25)

Default Configuration

The default VLAN last member query interval is 1 second.

Command Mode

Global Configuration mode

User Guidelines

In MLD snooping, when the IPv6 multicast router receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the router deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the router waits before deleting a non-responsive port from the multicast group. When a VLAN query interval is set, this interval overrides the global query interval. When the VLAN interval is set at 0, the global value is used.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 3 last-member-query-interval 30
```

ipv6 mld snooping vlan mrouter learn pim-dvmrp

To enable automatic learning of multicast router ports on the switch or on a VLAN, use the **ipv6 mld snooping vlan mrouter learn pim-dvmrp** Global Configuration mode command.

To disable this feature on the VLANs, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **mrouter learn pim-dvmrp**

no ipv6 mld snooping vlan *VLAN-LIST* **mrouter learn pim-dvmrp**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.

Default Configuration

MLD snooping learning pim-dvmrp is enabled.

Command Mode

Global Configuration mode

User Guidelines

multicast router ports are learned according to:

- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

ipv6 mld snooping vlan query-interval

To configure IPv6 MLD snooping query interval on the switch or on a VLAN, use the **ipv6 mld snooping vlan query-interval** Global Configuration mode command. This time interval is the maximum time that a multicast router waits after issuing an MASQ before deleting a port from the multicast group.

To revert to the default settings, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **query-interval** *VALUE*

no ipv6 mld snooping vlan *VLAN-LIST* **query-interval**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- *VALUE*—The IPv6 MLD snooping query interval. (Range: 30 to 18000)

Default Configuration

The default VLAN query interval is 125 seconds.

Command Mode

Global Configuration mode

User Guidelines

In MLD snooping, when the IPv6 multicast router receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the router deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the router waits before deleting a non-responsive port from the multicast group.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 7 query-interval 250
```

ipv6 mld snooping vlan response-time

To configure the Query Maximum Response time on the VLANs, use the **ipv6 mld snooping vlan response-time** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **response-time** *seconds*

no ipv6 mld snooping vlan *VLAN-LIST* **response-time**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- *seconds*—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5 to 20)

Default Configuration

10

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 3 response-time 20
```

ipv6 mld snooping vlan robustness-variable

To configure the number of IPv6 MLD queries that the switch sends before deleting a listener that does not respond, or to enter a VLAN ID to configure on a per-VLAN basis, use the **ipv6 mld snooping robustness-variable** Global Configuration mode command.

To revert to the default settings, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **robustness-variable** *VALUE*

no ipv6 mld snooping vlan *VLAN-LIST* **robustness-variable**

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- *VALUE*—The range is 1 to 7.

Default Configuration

The default VLAN robustness variable is 2.

Command Mode

Global Configuration mode

User Guidelines

Robustness is measured in terms of the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch waits before deleting a listener that does not respond and applies to all VLANs that do not have a VLAN value set.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 7 robustness-variable 5
```

ipv6 mld snooping vlan static interface

To enable the MLD snooping static group processing on a VLAN, use the **ipv6 mld snooping vlan static interface** Global Configuration mode command.

To disable this feature on the VLAN, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **static** *IPv6-Addr* **interface** *interface-id*

no ipv6 mld snooping vlan *VLAN-LIST* **static** *IPv6-Addr* **interface** *interface-id*

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- *IPv6-Addr*—The IPv6 multicast address.
- *interface-id*—The interface ID, which can be one of these types: Ethernet port or port channel.

Default Configuration

No ports are configured as a member of a multicast group.

Command Mode

Global configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Using the **no** command without a port list removes the entry.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 static abcd::1234 interface
fa1
```

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 static abcd::1234 interface
gi1
switchxxxxxx(config)# ipv6 mld snooping vlan 1 static abcd::1234 interface
po3
```

ipv6 mld snooping vlan mrouter

To register a Layer 2 port as a member of a static multicast group to the bridge table, use the **ipv6 mld snooping vlan mrouter** Global Configuration mode command.

To remove the ports specified as members from a static Mrouter port, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **mrouter interfaces** *interface-id*

no ipv6 mld snooping vlan *VLAN-LIST* **mrouter interfaces** *interface-id*

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No port is configured as a member of a static Mrouter port.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no** command without a port list removes the entry.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter interfaces fa1
```

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter interfaces gi1
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter interfaces po3
```

ipv6 mld snooping vlan forward-all

To enable the MLD snooping forward-all static port processing on a VLAN, use the **ipv6 mld snooping vlan forward-all** Global Configuration mode command.

To disable this feature on the VLAN, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **forward-all interfaces** *interface-id*

no ipv6 mld snooping vlan *VLAN-LIST* **forward-all interfaces** *interface-id*

Parameters

- *VLAN-LIST*—A VLAN ID or a list of VLAN IDs.
- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Default Configuration

No port is configured as a member of a multicast group.

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no** command without a port list removes the entry.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forward-all interfaces fa1
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forward-all interfaces gi1
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forward-all interfaces po1
```

profile range

To create a MLD profile for a range of IPv6 addresses, use the **profile range** MLD-profile Configuration mode command.

To remove a MLD profile for a range of IPv6 addresses, use the **no** form of this command.

Syntax

profile range ipv6 *ipv6-range* **action** {**deny** | **permit**}

Parameters

- **ipv6** *ipv6-range*—Specifies a range of IPv6 addresses for the profile. This can be a single IPv6 address or a range with a start and an end address. When entering a range, enter the low IPv6 multicast address, a space, and the high IPv6 multicast address.
- **action deny**—Denies the matching addresses.
- **action permit**—Permits the matching addresses.

Default Configuration

N/A

Command Mode

MLD-profile Configuration mode

Example

```
switchxxxxxx(config)# ip igmp profile 1
switchxxxxxx(config-mld-profile)# profile range ipv6 ff07::1:3 ff07::1:ff
action permit
```

show ipv6 mld filter

To display the IPv6 MLD profiles for all interfaces or for a specific interface, use the **show ipv6 mld filter** Privileged EXEC mode command.

Syntax

show ipv6 mld filter [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id* —(Optional) Specifies an interface ID or a list of interface IDs.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6 mld filter
Port ID  |  Profile ID
---------+--------------
     fa1 : None
     fa2 : 1
     fa3 : 1
     fa4 : 2
     fa5 : None
     fa6 : None
     fa7 : None
     fa8 : None
     fa9 : None
    fa10 : None
    fa11 : None
    fa12 : None
    fa13 : None
    fa14 : None
    fa15 : None
    fa16 : None
    fa17 : None
    fa18 : None
    fa19 : None
    fa20 : None
    fa21 : None
    fa22 : None
    fa23 : None
    fa24 : None
     gi1 : None
     gi2 : None
     po1 : None
     po2 : None
```

```
     po3 : None
     po4 : None
     po5 : None
     po6 : None
     po7 : None
     po8 : None
```

show ipv6 mld max-group

To display the maximum number of IPv6 MLD groups on a specific interface or all interfaces, use the **show ipv6 mld max-group** Privileged EXEC mode command.

Syntax

show ipv6 mld max-group [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

If no interface is specified, the information for all interfaces is displayed.

Example

```
switchxxxxxx# show ipv6 mld max-group interfaces fa5
Port ID   |  Max Group
---------+--------------
     fa5 : 512
```

show ipv6 mld max-group action

To display the action for a specific interface or for all interfaces when the number of IPv6 MLD groups exceeds the maximum group number, use the **show ipv6 mld max-group action** Privileged EXEC mode command.

Syntax

show ipv6 mld max-group action [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interfaces can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

If no interface is specified, the information for all interfaces is displayed.

Example

```
switchxxxxxx# show ipv6 mld max-group action interfaces fa5
Port ID  |  Max-groups  Action
---------+--------------------
     fa5 : deny
```

show ipv6 mld profile

To display the IPv6 MLD profile information, use the **show ipv6 mld profile** Privileged EXEC mode command.

Syntax

show ipv6 mld profile [*profile-index*]

Parameters

- *profile-index*—(Optional) The MLD profile index.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6 mld profile
IPv6 mld profile index: 1
IPv6 mld profile action: deny
Range low ip: ff51::
Range high ip: ff52::
```

show ipv6 mld snooping

To display the MLD snooping configuration, use the **show ipv6 mld snooping** Privileged EXEC mode command.

Syntax

show ipv6 mld snooping

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6 mld snooping


              MLD Snooping Status
                 --------------------

    Snooping                        : Disabled
    Report Suppression              : Enabled
    Operation Version               : v1
    Forward Method                  : mac
    Unknown Multicast Action        : Flood


                  Packet Statistics
```

```
Total RX                          :  0
Valid RX                          :  0
Invalid RX                        :  0
Other RX                          :  0
Leave RX                          :  0
Report RX                         :  0
General Query RX                  :  0
Special Group Query RX            :  0
Special Group & Source Query RX   :  0
Leave TX                          :  0
Report TX                         :  0
General Query TX                  :  0
Special Group Query TX            :  0
Special Group & Source Query TX   :  0
```

show ipv6 mld snooping forward-all

To display information for IPv6 MLD snooping forward all, use the **show ipv6 mld snooping forward-all** Privileged EXEC mode command.

Syntax

show ipv6 mld snooping forward-all [**vlan** *VLAN_LIST*]

Parameters

- **vlan** *VLAN-LIST*—(Optional) Specifies a VLAN ID or a list of VLAN IDs.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6 mld snooping forward-all

MLD Snooping VLAN           : 1
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 2
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 3
MLD Snooping static port    : None
MLD Snooping forbidden port : None
```

```
MLD Snooping VLAN           : 4
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 5
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 6
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 7
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 8
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 9
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 10
MLD Snooping static port    : None
MLD Snooping forbidden port : None
```

show ipv6 mld snooping groups

To display multicast groups learned by MLD snooping, use the **show ipv6 mld snooping groups** Privileged EXEC mode command.

Syntax

show ipv6 mld snooping groups [{**dynamic** | **static**} | *counters*]

Parameters

- **dynamic**—(Optional) Displays the dynamic groups.
- **static**—(Optional) Displays the static groups.
- *counters*—(Optional) IPv6 MLD snooping group counters.

Command Mode

Privileged EXEC mode

User Guidelines

To display information for all multicast groups learned by MLD snooping, use the **show ipv6 mld snooping groups** command without parameters.

To display information for a subset of all multicast groups learned by MLD snooping, use the **show ipv6 mld snooping groups** command with parameters.

Example

```
switchxxxxxx# show ipv6 mld snooping groups
VLAN  | Group IP Address |  Type   | Life(Sec) | Port
------+------------------+--------+-----------+------------------
Total Number of Entry = 0
```

show ipv6 mld snooping mrouter

To display information for dynamically, static, or forbidden learned multicast router port for all VLANs or for a specific VLAN, use **show ipv6 mld snooping mrouter** Privileged EXEC mode command.

Syntax

show ipv6 mld snooping mrouter [**dynamic** | **static** | **forbidden**]

Parameters

- **dynamic**—(Optional) Displays the dynamic groups.
- **forbidden**—(Optional) Displays the forbidden routers.
- **static**—(Optional) Displays the static groups.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6 mld snooping mrouter
Dynamic Mrouter Table
 VID   |  Port   | Expiry Time(Sec)
------+--------+-----------------
Total Entry 0
```

```
Static Mrouter Table
 VID    | Port Mask
------+-----------------------
Total Entry 0
Forbidden Mrouter Table
 VID    | Port Mask
------+-----------------------
Total Entry 0
```

show ipv6 mld snooping vlan

To display the MLD snooping configuration on specific VLANs, use the **show ipv6 mld snooping vlan** Privileged EXEC mode command.

Syntax

show ipv6 mld snooping vlan [*VLAN-LIST*]

Parameters

- *VLAN-LIST*—(Optional) A VLAN ID or a list of VLAN IDs.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ipv6 mld snooping vlan 100
MLD Snooping is globally enabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper mode : disabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper 10 sec
MLD Snooping last member query counter: admin 2  oper 2
MLD Snooping last member query interval: admin 1000 sec  oper 1000 sec
MLD Snooping last immediate leave: disabled
MLD Snooping automatic learning of mrouter ports: enabled
```

20

LACP Commands

lacp port-priority

To set the Link Aggregation Control Protocol (LACP) priority for an interface, use the **lacp port-priority** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

lacp port-priority *VALUE*

no lacp port-priority

Parameters

- *VALUE*—The LACP priority value for an interface. (Range: 1 to 65535)

Default Configuration

The default LACP port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi6
switchxxxxxx(config-if)# lacp port-priority 247
```

lacp system-priority

To set the global LACP priority for all interfaces, use the **lacp system-priority** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

lacp system-priority *VALUE*

no lacp system-priority

Parameters

- *VALUE*—The LACP priority value for all interfaces. (Range: 1 to 65535)

Default Configuration

The default LACP system priority is 32768.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lacp system-priority 120
```

lacp timeout

To assign an administrative LACP timeout to an interface, use the **lacp timeout** Interface Configuration mode command.

Syntax

lacp timeout {**long** | **short**}

Parameters

- **long**—Specifies that the periodic transmissions of LACP PDUs occur at a slow transmission rate.

- **short**—Specifies that the periodic transmissions of LACP PDUs occur at a fast transmission rate.

Default Configuration

The default timeout is **long**.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example assigns a long administrative LACP timeout to fa6:

```
switchxxxxxx(config)# interface gi6
switchxxxxxx(config-if)# lacp timeout long
```

show lacp

To show LACP channel-group information, use the **show lacp** Privileged EXEC mode command.

Syntax

show lacp sys-id

show lacp [*channel-group-number*] **counters**

show lacp [*channel-group-number*] {**internal** | **neighbor**} [**detail**]

Parameters

- **sys-id**—Displays the system identifier that is being used by LACP. The system identifier is made up of the LAPC system priority and the switch MAC address.
- *channel-group-number*—(Optional) Number of the channel group. The range is 1 to 8.
- **counters**—Displays traffic information.
- **internal**—Displays internal information.
- **neighbor**—Displays neighbor information.

- **detail**—(Optional) Displays detailed information.

Command Mode

Privileged EXEC Mode

User Guidelines

You can enter any **show lacp** command to display the active channel-group information.

To show information for a specific channel, enter the **show lacp** command with a channel-group number. If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

Examples

Example 1—The following example shows the LACP statistics:

```
switchxxxxxx# show lacp counters
             LACPDUs        LACPDUs
Port        Sent    Recv      Pkts Err
---------------------------------------
Channel group 1
fa1         5       3         0
fa2         8       0         0
Channel group 2
fa3         3       5         0
fa4         0       0         0
```

The following table describes the significant fields shown in the example:

Field	Description
Port	Port identifier.
LACPDUs Sent and Recv	Number of LACP packets sent and received by a port.
LACPDUs Pkts and Err	Number of unknown and illegal packets received by LACP for a port.

Example 2—The following example shows the LACP internal information:

```
switchxxxxxx# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 1
                              LACP port     Admin     Oper    Port        Port
Port      Flags   State       Priority      Key       Key     Number      State
fa1       SA      bndl        1             0x3e8     0x3e8   0x1         0x3d
fa2       SA      down        1             0x3e8     0x3e8   0x2         0x45

Channel group 2
                              LACP port     Admin     Oper    Port        Port
Port      Flags   State       Priority      Key       Key     Number      State
fa3       SA      bndl        1             0x3e9     0x3e9   0x3         0x3d
fa4       SA      down        1             0x3e9     0x3e9   0x4         0x45
```

The following table describes the significant fields shown in the example:

Field	Description
State	State of the specific port. The available values are: ▪ **bndl**—Port is attached to an aggregator and bundled with other ports. ▪ **susp**—Port is in a suspended state; it is not attached to any aggregator. ▪ **hot-sby**—Port is in a hot-standby state. ▪ **1indiv**—Port is incapable of bundling with any other port. ▪ **1indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). ▪ **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Field	Description
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port identifier.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: ▪ **bit0**—LACP_Activity ▪ **bit1**—LACP_Timeout ▪ **bit2**—Aggregation ▪ **bit3**—Synchronization ▪ **bit4**—Collecting ▪ **bit5**—Distributing ▪ **bit6**—Defaulted ▪ **bit7**—Expired **NOTE** In the list above, bit7 is the MSB and bit0 is the LSB.

Example 3—The following example shows the LACP neighbor details:

```
switchxxxxxx# show lacp neighbor detail

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 1
```

```
Partner's information


          Partner               Partner                      Partner
Port      System ID             Port Number     Age          Flags
gi13      32768, 00e0.4c86.7001 0x1             90s          SA

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          1                     0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes             Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No

          Partner               Partner                      Partner
Port      System ID             Port Number     Age          Flags
gi14      32768, 00e0.4c86.7001 0x2             63s          SA

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          1                     0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes             Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No

          Partner               Partner                      Partner
Port      System ID             Port Number     Age          Flags
gi15      32768, 00e0.4c86.7001 0x3             90s          SA

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          1                     0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes             Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No
```

Example 4—The following example shows the LACP system identifier information:

```
switchxxxxxx# show lacp sys-id
```

```
32768, 00e0.4c86.7001
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

21

Line Commands

clear line

To disconnect Telnet or SSH sessions, use the **clear line** Privileged EXEC Mode command.

Syntax

clear line {**ssh** | **telnet**}

Parameters

- **ssh**—Disconnects SSH sessions.
- **telnet**—Disconnects Telnet sessions.

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# clear line telnet
```

exec-timeout

To set the session idle time, during which the switch waits for user input before automatic logoff, use the **exec-timeout** Line Configuration mode command.

To revert to the default setting, use the **no** form of this command.

Syntax

exec-timeout *minutes*

no exec-timeout

Parameters

- *minutes*—The number of minutes. (Range: 0 to 65535, 0 means no timeout)

Default Configuration

The default idle time is 10 minutes.

Command Mode

Line Configuration mode

Example

The following example sets the idle time for Telnet sessions to 20 minutes:

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# exec-timeout 20
```

line

To identify a specific line for configuration and enter the Line Configuration command mode, use the **line** Global Configuration mode command.

Syntax

line {**console** | **ssh** | **telnet**}

Parameters

- **console**—Specifies the terminal line mode.
- **telnet**—Specifies the switch as a virtual terminal for remote access (Telnet).
- **ssh**—Specifies the switch as a virtual terminal for secured remote access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the switch as a virtual terminal for remote access (Telnet):

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

password-thresh

To set the login password intrusion threshold, use the **password-thresh** Line Configuration mode command.

Syntax

password-thresh *value*

Parameters

- *value*—The number of allowed password attempts. (Range: 0 to 120, 0 indicates no threshold)

Default Configuration

The default threshold value is 0, which indicates no threshold.

Command Mode

Line Configuration mode

Example

```
switchxxxxxx(config)# line console
switchxxxxxx (config-line)# password-thresh 10
```

show line

To show the line parameters, use the **show line** Privileged EXEC mode command.

Syntax

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

Parameters

- **console**—(Optional) Displays the console configuration.
- **telnet**—(Optional) Displays the Telnet configuration.
- **ssh**—(Optional) Displays the SSH configuration.

Default Configuration

If the line is not specified, all line configuration parameters are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays all line configuration parameters:

```
switchxxxxxx# show line
Console ================================
    Baudrate         : 9600
    Session Timeout  : 10 (minutes)
    History Count    : 128
    Password Retry   : 3
    Silent Time      : 0 (seconds)
Telnet =================================
    Telnet Server    : enabled
    Session Timeout  : 0 (minutes)
    History Count    : 128
    Password Retry   : 3
    Silent Time      : 0 (seconds)
SSH ====================================
    SSH Server       : disabled
    Session Timeout  : 10 (minutes)
    History Count    : 128
    Password Retry   : 3
    Silent Time      : 0 (seconds)
```

silent-time

To set the login fail silent time, use the **silent-time** Line Configuration mode command.

Syntax

silent-time *value*

Parameters

- *value*—The number of seconds to disable the console after login failure. (Range: 0 to 65535. 0 indicates no silent-time)

Default Configuration

No silent time

Command Mode

Line Configuration mode

Example

```
switchxxxxxx(config)# line console
switchxxxxxx (config-line)# silent-time 10
```

speed

To set the console port baud rate, use the **speed** Line Configuration mode command.

To revert to the default setting, use the **no** form of this command.

Syntax

speed *bps*

no speed

Parameters

- *bps*—The baud rate in bits per second (bps). Possible values are 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.

Default Configuration

The default console port baud rate is 9600 bps.

Command Mode

Line Configuration mode

User Guidelines

The configured speed is applied when autobaud is disabled. This configuration applies to the current session only.

Example

The following example sets the console baud rate to 115200 bps:

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# speed 115200
```

22

LLDP Commands

clear lldp statistics

To clear the Link Layer Discovery Protocol (LLDP) statistics, use the **clear lldp statistics** Privileged EXEC mode command.

Syntax

clear lldp statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear lldp statistics
```

lldp holdtime-multiplier

To specify how long the receiving device holds a LLDP packet before discarding it, use the **lldp holdtime-multiplier** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

lldp holdtime-multiplier *number*

no lldp holdtime-multiplier

Parameters

- *number*—The amount of time that LLDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. (Range: 2 to 10)

Default Configuration

The default LLDP holdtime multiplier is 4.

Command Mode

Global Configuration mode

User Guidelines

The time-to-live (TTL) value (the LLDP transmission interval multiplies the holdtime multiplier) should be smaller than 65535.

The actual TTL value of LLDP frames is calculated by the following formula:

TTL = min (65535, LLDP-Timer * LLDP-hold-multiplier)

For example, if the value of the LLDP timer is 30 seconds, and the value of the LLDP holdtime multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.

Example

The following example sets the LLDP holdtime interval to 90 seconds:

```
switchxxxxxx(config)# lldp timer 30
switchxxxxxx(config)# lldp holdtime-multiplier 3
```

lldp lldpdu

To specify how to handle LLDP packets when LLDP is globally disabled, use the **lldp lldpdu** Global Configuration mode command.

Syntax

lldp lldpdu {**bridging** | **filtering** | **flooding**}

Parameters

- **bridging**—Bridges LLDP packets (bridging LLDP PDU to VLAN member ports) when LLDP is globally disabled.
- **filtering**—Filters (deletes) LLDP packets when LLDP is globally disabled.
- **flooding**—Floods (forwards) LLDP packets to all interfaces when LLDP is globally disabled.

Default Configuration

LLDP packets are flooded when LLDP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

If the STP mode is set to MSTP, the LLDP packet-handling mode cannot be set to flooding. The STP mode cannot be set to MSTP if the LLDP packet-handling mode is flooding. If LLDP is globally disabled, and the LLDP packet-handling mode is flooding, LLDP packets are treated as data packets with the following exceptions:

- VLAN ingress rules are not applied to LLDP packets. LLDP packets are trapped on all ports for which the STP state is Forwarding.
- Default deny-all rules are not applied to LLDP packets.
- VLAN egress rules are not applied to the packets. LLDP packets are flooded to all ports for which the STP state is Forwarding.
- LLDP packets are sent as untagged.

Example

```
switchxxxxxx(config)# lldp lldpdu flooding
```

lldp med

To enable LLDP Media Endpoint Discovery (MED) on an interface, use the **lldp med** Interface Configuration mode command.

To disable LLDP MED on an interface, use the **no** form of this command.

Syntax

lldp med {**enable** | **disable**}

no lldp med

Parameters

- **enable**—Enables LLDP MED on the interface.
- **disable**—Disables LLDP MED on the interface.

Default Configuration

LLDP MED is enabled with the network-policy TLV.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# lldp med enable
```

lldp med fast-start-repeat-count

When an interface comes up, LLDP can send packets more quickly than usual using its fast start mechanism. To configure the number of packets that is sent during the activation of the fast start mechanism, use the **lldp med fast-start-repeat-count** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

lldp med fast-start-repeat-count *number*

no lldp med fast-start-repeat-count

Parameters

- *number*—The number of times that the fast start LLDPDU is being sent during the activation of the fast start mechanism. (Range: 1 to 10)

Default Configuration

The default value is 3.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp med fast-start-repeat-count 4
```

lldp med location

To configure the LLDP MED location for an interface, use the **lldp med location** Interface Configuration mode command.

To remove the LLDP MED location for an interface, use the **no** form of this command.

Syntax

lldp med location {**civic-address** *data* | **coordinate** *data* | **ecs-elin** *data*}

no lldp med location {**civic-address** | **coordinate** | **ecs-elin**}

Parameters

- **civic-address** *data*—Specifies the location data as a civic address in hexadecimal format.
- **coordinate** *data*—Specifies the location data as coordinates in hexadecimal format.
- **ecs-elin** *data*—Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN) in hexadecimal format.

Default Configuration

The location is not configured.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# lldp med location civic-address 616263646566
```

lldp med network-policy voice auto

To automatically create an LLDP MED network policy for voice application, if the voice VLAN operation mode is auto voice VLAN, use the **lldp med network-policy auto** Global Configuration mode command. The voice VLAN, 802.1p priority, and the DSCP value of the voice VLAN are used in the policy.

To disable this feature, use the **no** form of this command.

Syntax

lldp med network-policy voice auto

no lldp med network-policy voice auto

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

A network policy for voice LLDP packets can be created by using the **lldp med network-policy (global)** command. The **lldp med network-policy auto** Global Configuration mode command allows you to use the configuration of the voice application to create the network policy instead of having to manually configure it.

In the Auto mode, the voice VLAN feature determines on which interfaces to advertise the network policy TLV with the application type **voice**, and controls the parameters of that TLV.

To enable auto generation of a network policy based on the auto voice VLAN, there must be no manual preconfigured network policies for the voice application. In the Auto mode, you cannot manually define a network policy for the voice application using the **lldp med network-policy (global)** command.

Example

```
switchxxxxxx(config)# lldp med network-policy voice auto
```

lldp med network-policy (Global)

To manually define an LLDP MED network policy, use the **lldp med network-policy** Global Configuration mode command.

To delete an LLDP MED network policy, use the **no** form of this command.

Syntax

lldp med network-policy *number* **app** {**voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **softphone-voice** | **streaming-video** | **video-conferencing** | **video-signaling**} **vlan** *vlan-id* **vlan-type** { **tag** | **untag** } **priority** *priority* **dscp** *value*

no lldp med network-policy *number*

Parameters

- *number*—Network policy index number. (Range: 1 to 32)
- **app**—Specifies the type of the application defined for this network policy. Available application types are:
  - voice

- voice-signaling
- guest-voice
- guest-voice-signaling
- softphone-voice
- video-conferencing
- streaming-video
- video-conferencing
- video-signaling

- **vlan** *vlan-id*—Specifies the VLAN identifier for the application.
- **vlan-type** {**tag** | **untag**} —Specifies if the application is using a tagged or an untagged VLAN.
- **priority** *priority*—Specifies the user priority used for the specified application.
- **dscp** *value*—Specifies the DSCP value used for the specified application.

Default Configuration

No network policy is defined.

Command Mode

Global Configuration mode

User Guidelines

This command creates the network policy, which can be attached to a port by using the **lldp med network-policy (interface)** command.

Use the **lldp med network-policy** Interface Configuration mode command to attach a network policy to a port.

Up to 32 network policies can be defined.

Example

This example creates a network policy for the voice-signaling application and attaches it to gi1. LLDP packets sent on gi1 will contain information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 app voice-signaling vlan 1
vlan-type untagged priority 1 dscp 2
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

lldp med network-policy (Interface)

To attach (or remove) an LLDP MED network policy to (or from) an interface, use the **lldp med network-policy** Interface Configuration mode command.

Syntax

lldp med network-policy {**add** | **remove**} *number*

Parameters

- **add** *number*—Attaches the specified network policy to the interface.
- **remove** *number*—Removes the specified network policy to the interface.

Default Configuration

No network policy is attached to the interface.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

For each interface, only one network policy per application can be defined. Network policies are created by using the **lldp med network-policy (global)** command.

Example

This example creates a network policy for the voice-signaling application and attaches it to fa1 1. LLDP packets sent on fa1 1 will contain information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 app voice-signaling vlan 2
vlan-type untag priority 1 dscp 2
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# lldp med network-policy add 1
```

lldp med tlv-select

To specify which LLDP MED TLVs are included, use the **lldp med tlv-select** Interface Configuration mode command.

To remove all selected LLDP MED TLVs, use the **no** form of this command.

Syntax

lldp med tlv-select *medtlv1* [*medtlv2... medtlv4*]

no lldp med tlv-select

Parameters

- *medtlv*—TLVs that should be included or excluded. Available TLVs are network-policy, location, poe-pse, and inventory. The capabilities TLV is always included if LLDP MED is enabled.

Default Configuration

Network-policy TLV

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables LLDP MED with the location TLV on gi5:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# lldp med tlv-select location
```

lldp receive

To enable receiving LLDP frames on an interface, use the **lldp receive** Interface Configuration mode command.

To stop receiving LLDP frames on an interface, use the **no** form of this command.

Syntax

lldp receive

no lldp receive

Parameters

N/A

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

LLDP manages LAG ports individually. LLDP data received through the LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. For example, LLDP frames are received on the blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# lldp receive
```

lldp reinit

To specify the minimum time that an LLDP-enabled port waits before reinitializing the LLDP transmission, use the **lldp reinit** Global Configuration mode command.

To revert to its default settings, use the **no** form of this command.

Syntax

lldp reinit *seconds*

no lldp reinit

Parameters

- *seconds*—The minimum time in seconds that a LLDP port waits before reinitializing the LLDP transmission. (Range: 1 to 10)

Default Configuration

2 seconds

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp reinit 4
```

lldp run

To enable LLDP globally on the switch, use the **lldp run** Global Configuration mode command.

To disable LLDP globally on the switch, use the **no** form of this command.

Syntax

lldp run

no lldp run

Parameters

N/A

Default Configuration

LLDP is enabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp run
```

lldp tlv-select 802.1

To specify which 802.1x parameters will be advertised, use the **lldp tlv-select 802.1** Interface Configuration mode command.

Syntax

lldp tlv-select 802.1 pvid enable

lldp tlv-select 802.1 pvid disable

lldp tlv-select 802.1 vlan-name add *vlan-id*

lldp tlv-select 802.1 vlan-name remove *vlan-id*

Parameters

- **pvid enable**—Specifies that the PVID is advertised.
- **pvid disable**—Specifies that the PVID is not advertised.
- **vlan-name add** *vlan-id*—Specifies that the VLAN ID is advertised. (Range: 1 to 4094)
- **vlan-name remove** *vlan-id*—Specifies that the VLAN ID is not advertised. (Range: 1 to 4094)

Default Configuration

802.1 pvid TLV is transmitted.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# lldp tlv-select 802.1 pvid enable
```

lldp tlv-select TLV

To specify which optional TLVs are transmitted, use the **lldp tlv-select TLV** Interface Configuration (Ethernet) mode command.

To remove all selected LLDP optional TLVs, use the **no** form of this command.

Syntax

lldp tlv-select *TLV* [*TLV*] [*TLV*] [*TLV*] [*TLV*] [*TLV*] [*TLV*] [*TLV*]

no lldp tlv-select

Parameters

- *TLV*—(Optional) Available optional TLVs are port-desc, sys-name, sys-desc, sys-cap, mac-phy, lag, max-frame-size, and management-addr.

Default Configuration

The sys-name and sys-cap TLVs are selected.

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi20
switchxxxxxx(config-if)# lldp tlv-select port-desc sys-name sys-desc
```

lldp transmit

To enable transmitting LLDP frames on an interface, use the **lldp transmit** Interface Configuration mode command.

To stop transmitting LLDP frames on an interface, use the **no** form of this command.

Syntax

lldp transmit

no lldp transmit

Parameters

N/A

Default Configuration

Transmitting LLDP is enabled on each interface.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG.

LLDP operation on a port is not dependent on the STP state of a port. For example, LLDP frames are sent on the blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# lldp transmit
```

lldp tx-delay

To set the delay time between two successive LLDP frame transmissions initiated by value or status changes in the LLDP local system MIB, use the **lldp tx-delay** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

lldp tx-delay *seconds*

no lldp tx-delay

Parameters

- *seconds*—The delay time in seconds. (Range: 1 to 8191 seconds)

Default Configuration

The default delay time is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

We recommend that the tx-delay is less than 0.25 of the LLDP timer interval.

Example

```
switchxxxxxx(config)# lldp tx-delay 10
```

lldp timer

To specify how often the system sends the LLDP updates, use the **lldp timer** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

lldp timer *seconds*

no lldp timer

Parameters

- *seconds*—The minimum time in seconds that an LLDP port transmits the advertisement periodically. (Range: 5 to 32767)

Default Configuration

30 seconds

Command Mode

Global Configuration mode

User Guidelines

LLDP transmission interval multiplies the holdtime multiplier should be smaller than 65535.

The tx-delay cannot be larger than 0.25 of the LLDP transmission interval.

Example

```
switchxxxxxx(config)# lldp timer 30
```

show lldp

To show the LLDP status, use the **show lldp** Privileged EXEC mode command.

Syntax

show lldp

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show lldp

 State: Enabled
 Timer: 30 Seconds
 Hold multiplier: 4
 Reinit delay: 2 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Flooding

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi1 |  RX,TX |         SN, SC |192.168.1.254
      gi2 |  RX,TX |         SN, SC |192.168.1.254
      gi3 |  RX,TX |         SN, SC |192.168.1.254
      gi4 |  RX,TX |         SN, SC |192.168.1.254
      gi5 |  RX,TX |         SN, SC |192.168.1.254
      gi6 |  RX,TX |         SN, SC |192.168.1.254
      gi7 |  RX,TX |         SN, SC |192.168.1.254
      gi8 |  RX,TX |         SN, SC |192.168.1.254
      gi9 |  RX,TX |         SN, SC |192.168.1.254
     gi10 |  RX,TX |         SN, SC |192.168.1.254
     gi11 |  RX,TX |         SN, SC |192.168.1.254
```

```
      gi12 |  RX,TX |          SN, SC |192.168.1.254
      gi13 |  RX,TX |          SN, SC |192.168.1.254
      gi14 |  RX,TX |          SN, SC |192.168.1.254
      gi15 |  RX,TX |          SN, SC |192.168.1.254
      gi16 |  RX,TX |          SN, SC |192.168.1.254
      gi17 |  RX,TX |          SN, SC |192.168.1.254
      gi18 |  RX,TX |          SN, SC |192.168.1.254
      gi19 |  RX,TX |          SN, SC |192.168.1.254
      gi20 |  RX,TX |          SN, SC |192.168.1.254
      gi21 |  RX,TX |          SN, SC |192.168.1.254
      gi22 |  RX,TX |          SN, SC |192.168.1.254
      gi23 |  RX,TX |          SN, SC |192.168.1.254
      gi24 |  RX,TX |          SN, SC |192.168.1.254
      gi25 |  RX,TX |          SN, SC |192.168.1.254
      gi26 |  RX,TX |          SN, SC |192.168.1.254
      gi27 |  RX,TX |          SN, SC |192.168.1.254
      gi28 |  RX,TX |          SN, SC |192.168.1.254

Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi3
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi4
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi5
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi6
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi7
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi8
802.3 optional TLVs:
```

```
802.1 optional TLVs
PVID: Enabled

Port ID: gi9
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi10
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi11
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi12
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi13
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi14
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi15
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi16
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi17
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi18
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi19
802.3 optional TLVs:
```

```
802.1 optional TLVs
PVID: Enabled

Port ID: gi20
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi21
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi22
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi23
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi24
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi25
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi26
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi27
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled

Port ID: gi28
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

show lldp interfaces

To show the LLDP configuration for specific interfaces, use the **show lldp interfaces** Privileged EXEC mode command.

Syntax

show lldp interfaces *interface-id*

Parameters

- *interface-id*—An interface ID or a list of interface IDs.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show lldp interfaces gi11

 State: Enabled
 Timer: 30 Seconds
 Hold multiplier: 4
 Reinit delay: 2 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Flooding

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
     gi11 |  RX,TX |          SN, SC |192.168.1.254

Port ID: gi11
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

show lldp interfaces tlvs-overloading

To show the status of LLDP TLVs overloading for specific interfaces, use the **show lldp interfaces tlvs-overloading** Privileged EXEC mode command.

Syntax

show lldp interfaces *interface-id* **tlvs-overloading**

Parameters

- *interface-id*—An interface ID or a list of interface IDs.

Command Mode

Privileged EXEC mode

User Guidelines

When an LLDP packet contains too much information for one packet, this is called overloading.

The command calculates the overloading status of the current LLDP configuration, not for the last LLDP packet that was sent.

Example

```
switchxxxxxx# show lldp interfaces gi11 tlvs-overloading

gi11:

          TLVs Group           |  Bytes  |      Status
 ----------------------------- + ------- + ----------------
                     Mandatory |      22 |    Transmitted
        LLDP-MED Capabilities  |       9 |    Transmitted
    LLDP-MED Network Policies  |      10 |    Transmitted
                      Optional |      20 |    Transmitted
                         802.1 |       8 |    Transmitted

Total: 69 bytes
Left: 1419 bytes
```

show lldp local-device

To show LLDP information that is advertised from specific interfaces, use the **show lldp local-device** Privileged EXEC mode command.

Syntax

show lldp [**interfaces** *interface-id*] **local-device**

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. If not specified, the command displays some common information of local device.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays the LLDP local device information that is advertised from fa1 1:

```
switchxxxxxx# show lldp interfaces gi11 local-device

Device ID: 00:E0:4C:86:70:01
Port ID: gi11
System Name: switchxxxxxx
Capabilities: Bridge
System description: 28-Port Gigabit PoE Smart Switch
Port description:
Time To Live: 120
802.1 PVID: 1
LLDP-MED capabilities: Capabilities, Network Policy
LLDP-MED Device type: Network Connectivity
```

Example 2—The following example displays the LLDP local device information:

```
switchxxxxxx# show lldp local-device

LLDP Local Device Information:
 Chassis Type : Mac Address
 Chassis ID   : DE:AD:BE:EF:01:02
 System Name  : SwitchEF0102
 System Description  :
 System Capabilities Support : Bridge
```

```
System Capabilities Enable  : Bridge
Management Address : 192.168.1.254(IPv4)
```

show lldp med

To display the LLDP MED configuration for specific interfaces, use the **show lldp med** Privileged EXEC mode command.

Syntax

show lldp [**interfaces** *interface-id*] **med**

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. If not specified, the command displays information for all interfaces.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example shows the LLDP MED configuration for all interfaces:

```
switchxxxxxx# show lldp med

Fast Start Repeat Count: 3
 lldp med network-policy voice: auto

 Port   | Capabilities  | Network Policy | Location | Inventory | POE
 ------ + ------------- + -------------- + -------- + ----------+ -----
    gi1 |           Yes |            Yes |       No |        No |   No
    gi2 |           Yes |            Yes |       No |        No |   No
    gi3 |           Yes |            Yes |       No |        No |   No
    gi4 |           Yes |            Yes |       No |        No |   No
    gi5 |           Yes |            Yes |       No |        No |   No
    gi6 |           Yes |            Yes |       No |        No |   No
    gi7 |           Yes |            Yes |       No |        No |   No
    gi8 |           Yes |            Yes |       No |        No |   No
    gi9 |           Yes |            Yes |       No |        No |   No
   gi10 |           Yes |            Yes |       No |        No |   No
   gi11 |           Yes |            Yes |       No |        No |   No
   gi12 |           Yes |            Yes |       No |        No |   No
   gi13 |           Yes |            Yes |       No |        No |   No
```

```
   gi14 |           Yes |           Yes |       No |        No |   No
   gi15 |           Yes |           Yes |       No |        No |   No
   gi16 |           Yes |           Yes |       No |        No |   No
   gi17 |           Yes |           Yes |       No |        No |   No
   gi18 |           Yes |           Yes |       No |        No |   No
   gi19 |           Yes |           Yes |       No |        No |   No
   gi20 |           Yes |           Yes |       No |        No |   No
   gi21 |           Yes |           Yes |       No |        No |   No
   gi22 |           Yes |           Yes |       No |        No |   No
   gi23 |           Yes |           Yes |       No |        No |   No
   gi24 |           Yes |           Yes |       No |        No |   No
   gi25 |           Yes |           Yes |       No |        No |   No
   gi26 |           Yes |           Yes |       No |        No |   No
   gi27 |           Yes |           Yes |       No |        No |   No
   gi28 |           Yes |           Yes |       No |        No |   No
```

Example 2—The following example shows the LLDP MED configuration for gi11:

```
switchxxxxxx# show lldp interfaces gi11 med

 Port   | Capabilities  | Network Policy | Location | Inventory | POE
 ------ + ------------- + -------------- + -------- + ----------+ -----
   gi11 |           Yes |            Yes |       No |        No |   No

Port ID: gi11
Network policies:
```

show lldp neighbor

To show information about neighboring devices discovered using LLDP, use the **show lldp neighbor** Privileged EXEC mode command.

Syntax

show lldp [**interfaces** *interface-id*] **neighbor**

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. If not specified, the command displays information for all interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

A TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

Example

```
switchxxxxxx# show lldp neighbor
Port | Device ID  |  Port ID   |  SysName      |  Capabilities  |  TTL
---- + ---------- + ---------- + ------------ + ------------ + -----
```

The following table describes the significant fields shown in the example:

Field	Description
Port	Local port number.
Device ID	The neighbor device's configured ID (name) or MAC address.
Port ID	The neighbor device's port ID.
SysName	The neighbor device's administratively assigned name.
Capabilities	The capabilities discovered on the neighbor device. Possible values are: ▪ B - Bridge ▪ R - Router ▪ W - WLAN Access Point ▪ T - Telephone ▪ D - DOCSIS cable device ▪ H - Host ▪ r - Repeater ▪ O - Other
TTL	Time interval in seconds after which the information for this neighbor is deleted.

show lldp statistics

To show the LLDP statistics for specific interfaces, use the **show lldp statistics** Privileged EXEC mode command.

Syntax

show lldp [**interfaces** *interface-id*] **statistics**

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. If not specified, the command displays information for all interfaces.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show lldp interfaces gi1-2 statistics

LLDP Port Statistics:
        | TX Frames |          RX Frames          |          RX TLVs          |
RX Ageouts
  Port  |   Total   | Total | Discarded | Errors | Discarded | Unrecognized |
Total
--------+-----------+-------+-----------+--------+-----------+--------------
+----------
    gi1 |         0 |     0 |         0 |      0 |         0 |            0 |
0
    gi2 |         0 |     0 |         0 |      0 |         0 |            0 |
0
```

The following table describes the significant fields shown in the example:

Field	Description
Port	Identifier of interface.
TX Frames Total	Total number of transmitted frames.
RX Frames Total	Total number of received frames.
RX Frames Discarded	Total number of received frames that were discarded.
RX Frames Errors	Total number of received frames with errors.

Field	Description
RX TLVs Discarded	Total number of received TLVs that were discarded.
RX TLVs Unrecognized	Total number of received TLVs that were unrecognized.
RX Ageouts Total	Number of neighbor age outs on the interface.

23

Loopback Detection Commands

loopback-detection enable (Global)

To enable the Loopback Detection (LBD) feature globally, use the **loopback-detection enable** Global Configuration mode command.

To disable the Loopback Detection feature, use the **no** form of this command.

Syntax

loopback-detection enable

no loopback-detection enable

Parameters

None.

Default Configuration

Loopback Detection is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **loopback-detection enable** command to globally enable loopback detection protocol. Use the no form of this command to disabled it.

You can verify your setting by entering the **show loopback-detection Privileged EXEC** command.

Example

The following example shows how to enable loopback-detection:

```
switchxxxxxx(config)#loopback-detection enable
```

```
switchxxxxxx(config)# do show loopback-detection
Loopback detection: Enabled
Loopback detection interval : 30

Interface Loopback Detection Loopback Detection
          Admin State        Operational Status
--------- ------------------ ------------------
fa1       disabled           inactive
fa2       disabled           inactive
fa3       disabled           inactive
```

loopback-detection enable (Interface)

To enable the Loopback Detection (LBD) feature on an interface, use the **loopback-detection enable** Interface (Ethernet, Port Channel) Configuration mode command.

To disable the Loopback Detection feature on the interface, use the **no** form of this command.

Syntax

loopback-detection enable

no loopback-detection enable

Parameters

None.

Default Configuration

Loopback Detection is enabled on an interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the **loopback-detection enable** command to globally enable loopback detection protocol on ports. Use the no form of this command to disabled it.

You can verify your setting by entering the **show loopback-detection Privileged EXEC** command.

Example

The following example shows how to enable loopback-detection:

```
switchxxxxxx(config)#interface fa1
switchxxxxxx(config-if)#loopback-detection enable
switchxxxxxx(config-if)# do show loopback-detection interfaces fa1
Loopback detection: Enabled
Loopback detection interval : 30

Interface Loopback Detection Loopback Detection
          Admin State        Operational Status
--------- ------------------ ------------------
fa1       enabled            inactive
```

loopback-detection interval

To set the time interval between LBD packets, use the **loopback-detection interval** Global Configuration mode command.

To restore the default configuration, use the **no** form of this command.

Syntax

loopback-detection interval *seconds*

no loopback-detection interval

Parameters

- *seconds*—Specifies the time interval in seconds between LBD packets. (Range: 1—60 seconds.)

Default Configuration

The default time interval between LBD packets is 30 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use the **loopback-detection interval** command to change broadcasting interval. Use the no form of this command to restore to default.

You can verify your setting by entering the **show loopback-detection Privileged EXEC** command.

Example

The following example shows how to enable loopback-detection:

```
switchxxxxxx(config)#loopback-detection interval 40
switchxxxxxx(config)# do show loopback-detection
Loopback detection: Enabled
Loopback detection interval : 40

Interface Loopback Detection Loopback Detection
          Admin State        Operational Status
--------- ------------------ ------------------
fa1       disabled           inactive
fa2       disabled           inactive
fa3       disabled           inactive
```

show loopback-detection

To show loopback-detection status, use the **show loopback-detection** Privileged EXEC mode command.

Syntax

show loopback-detection [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—Specifies an interface ID or a list of interface IDs.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Operational status of Active indicates that the following conditions are met:

- Loopback is globally enabled.

- Loopback is enabled on the interface.
- Interface operational state of the interface is up.
- Interface STP state is Forwarding or STP state is disabled.

Operational status of loopDetected indicates that the interface entered errDisabled state.

Operational status of Inactive indicates that loopback detection is not actively attempting to detect loops, (that is, the Active status conditions are not meet).

Example

This example shows how to show loopback-detection configuration:

```
switchxxxxxx(config)# loopback-detection enable
switchxxxxxx(config)# do show loopback-detection
Loopback detection: Enabled
Loopback detection interval : 30

Interface Loopback Detection Loopback Detection
          Admin State        Operational Status
--------- ------------------ ------------------
fa1       disabled           inactive
fa2       disabled           loopDetected
fa3       disabled           inactive
```

24

Management ACL Commands

deny (Management)

To set the deny rules (ACEs) for the management ACL, use the **deny** Management Access-List Configuration mode command.

Syntax

[**sequence** *sequence-number*] **deny interfaces** *interface-id* **service** *service*

[**sequence** *sequence-number*] **deny** {**ip** *ipv4-address*| *ipv4mask* | **ipv6** *ipv6-address*| *ipv6-prefix-length*} [**interfaces** *interface-id*] **service** *service*

Parameters

- **sequence** *sequence-number*—(Optional) Specifies the sequence number for the ACL statement. The acceptable range is from 1 to 65535. If not specified, the switch provides a number starting from 1 in ascending order.
- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.
- **service** *service*—Specifies the type of service. Possible values are all, Telnet, SSH, HTTP, HTTPS, and SNMP.
- **ip** *ipv4-address*| *ipv4-mask*—Specifies the source IPv4 address and mask address.
- **ipv6** *ipv6-address*| *ipv6-prefix-length*—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

The rules with Ethernet and port channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny ip 192.168.1.111/0.0.255.255 interfaces gi11
service http
switchxxxxxx(config-macl)# exit
```

management access-class

To restrict the management connections by defining the active management ACLs, use the **management access-class** Global Configuration mode command.

To disable the management connection restrictions, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

Parameters

- **console-only**—Specifies that the switch can be managed only from the console.
- *name*—The ACL name to be used.

Default Configuration

The default is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an ACL called mlist as the active management ACL:

```
switchxxxxxx(config)# management access-class mlist
switchxxxxxx(config-macl)# permit ip 192.168.1.111/0.0.255.255 interfaces gi9
service all
switchxxxxxx(config-macl)# permit ip 192.168.1.111/0.0.255.255 interfaces
gi11 service all
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

management access-list

To configure a management access control list (ACL) and enter the Management Access-List Configuration command mode, use the **management access-list** Global Configuration mode command.

To delete a management ACL, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

Parameters

- *name*—The ACL name.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management ACL. This command enters the Management Access-List Configuration command mode, where the denied or permitted access conditions are defined with the **deny** and **permit** commands.

If no match criteria is defined, the default value is **deny**.

When reentering the ACL context, the new rules are entered at the end of the access list.

Use the **management access-class** command to select the active management ACLs. The active management ACLs cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with the service field are ignored), and then again on the inner IPv6 header.

Example

Example 1—The following example creates a management ACL called mlist, configures fa9 and fa11 as the management interfaces, and adds the new ACL to the active ACL:

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit ip 192.168.1.111/0.0.255.255 interfaces gi9
service all
switchxxxxxx(config-macl)# permit ip 192.168.1.111/0.0.255.255 interfaces
gi11 service all
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

Example 2—The following example creates a management ACL called mlist, configures all interfaces to be management interfaces except fa9 and 11, and adds the new ACL to the active ACL:

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny ip 192.168.1.111/0.0.255.255 interfaces gi9
service all
switchxxxxxx(config-macl)# deny ip 192.168.1.111/0.0.255.255 interfaces gi11
service all
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

no sequence (Management)

To remove a permit or deny condition (ACE) for a specific management ACL, use the **no sequence** Management Access List Configuration mode command.

Syntax

no sequence

Parameters

N/A

Command Mode

Management Access List Configuration mode

Example

```
switchxxxxxx# show management access-list

2 management  access-lists are created

console-only
------------
  sequence 1 deny interfaces fa1-24,gi1-2,po1-8 service all
  ! (Note: all other access implicitly denied)


mgmtacl1
--------
  sequence 1 permit interfaces fa1 service telnet
  ! (Note: all other access implicitly denied)

switchxxxxxx# config
switchxxxxxx(config)# management access-list mgmtacl1
switchxxxxxx(config-macl)# no sequence 1
```

permit (Management)

To set the permit rules (ACEs) for the management ACL, use the **permit** Management Access-List Configuration mode command.

Syntax

[**sequence** *sequence-number*] **permit interfaces** *interface-id* **service** *service*

[**sequence** *sequence-number*] **permit** {**ip** *ipv4-address*| *ipv4mask* | **ipv6** *ipv6-address*| *ipv6-prefix-length*} [**interfaces** *interface-id*] **service** *service*

Parameters

- **sequence** *sequence-number*—(Optional) Specifies the sequence number for the ACL statement. The acceptable range is from 1 to 65535. If not specified, the switch provides a number starting from 1 in ascending order.
- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.
- **service** *service*—Specifies the type of service. Possible values are all, Telnet, SSH, HTTP, HTTPS, or SNMP.
- **ip** *ipv4-address/ipv4-mask*—Specifies the source IPv4 address and mask address.
- **ipv6** *ipv6-address/ipv6-prefix-length*—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

The rules with Ethernet, VLAN, and port channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit ip 192.168.1.111/0.0.255.255 interfaces
gi11 service http
switchxxxxxx(config-macl)# exit
```

show management access-class

To show information about the active management ACL, use the **show management access-class** Privileged EXEC mode command.

Syntax

show management access-class

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
```

show management access-list

To show information for all management ACLs or for a specific management ACL, use the **show management access-list** Privileged EXEC mode command.

Syntax

show management access-list [*name*]

Parameters

- *name*—(Optional) The name of a management ACL to be displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays information for all management ACLs:

```
switchxxxxxx# show management access-list

2 management  access-lists are created

console-only
------------
  sequence 1 deny interfaces fa1-24,gi1-2,po1-8 service all
  ! (Note: all other access implicitly denied)


mlist
-----
  sequence 1 permit interfaces fa11 service all
  ! (Note: all other access implicitly denied)
```

25

PHY Diagnostics Commands

show cable-diagnostics cable-length

To show the estimated copper cable length attached to a specific interface, use the **show cable-diagnostics cable-length** Privileged EXEC Mode command.

Syntax

show cable-diagnostics cable-length {**interfaces** *interface-id*}

Parameters

- **interfaces** *interface-id*—Specifies an Ethernet interface ID or a list of Ethernet interface IDs.

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

User Guidelines

The interface must be active and working at 100 Mbps or 1000 Mbps.

Example

```
switchxxxxxx# show cable-diagnostics cable-length interfaces gi1-24
 Port    |  Speed | Local pair | Pair length | Pair status
--------+--------+------------+-------------+---------------
  gi1    |  auto  |    Pair A  |     0.96    | Open
                     Pair B  |     0.93    | Open
                     Pair C  |     0.90    | Open
                     Pair D  |     0.83    | Open

  gi2    |  auto  |    Pair A  |     0.95    | Open
                     Pair B  |     0.90    | Open
                     Pair C  |     0.85    | Open
```

```
                                Pair D  |     0.83    | Open

 gi3    |  auto  |    Pair A  |     0.93    | Open
                     Pair B  |     0.91    | Open
                     Pair C  |     0.85    | Open
                     Pair D  |     0.85    | Open

 gi4    |  auto  |    Pair A  |     0.87    | Open
                     Pair B  |     0.91    | Open
                     Pair C  |     0.85    | Open
                     Pair D  |     0.82    | Open

 gi5    |  auto  |    Pair A  |     1.00    | Open
                     Pair B  |     0.91    | Open
                     Pair C  |     0.87    | Open
                     Pair D  |     0.90    | Open

 gi6    |  auto  |    Pair A  |     0.90    | Open
                     Pair B  |     0.90    | Open
                     Pair C  |     0.88    | Open
                     Pair D  |     0.87    | Open

 gi7    |  auto  |    Pair A  |     0.96    | Open
                     Pair B  |     0.95    | Open
                     Pair C  |     0.91    | Open
                     Pair D  |     0.90    | Open

 gi8    |  auto  |    Pair A  |     0.92    | Open
                     Pair B  |     0.93    | Open
                     Pair C  |     0.88    | Open
                     Pair D  |     0.88    | Open

 gi9    |  auto  |    Pair A  |     0.90    | Open
                     Pair B  |     0.90    | Open
                     Pair C  |     0.87    | Open
                     Pair D  |     0.85    | Open

gi10    |  auto  |    Pair A  |     0.86    | Open
                     Pair B  |     0.86    | Open
                     Pair C  |     0.83    | Open
                     Pair D  |     0.81    | Open

gi11    |  auto  |    Pair A  |     0.92    | Open
                     Pair B  |     0.91    | Open
                     Pair C  |     0.81    | Open
                     Pair D  |     0.83    | Open

gi12    |  auto  |    Pair A  |     0.86    | Open
                     Pair B  |     0.90    | Open
                     Pair C  |     0.82    | Open
                     Pair D  |     0.86    | Open

gi13    |  auto  |    Pair A  |     0.90    | Open
                     Pair B  |     0.92    | Open
                     Pair C  |     0.88    | Open
```

```
                          Pair D  |     0.87    | Open

gi14    |  auto  |        Pair A  |     0.91    | Open
                          Pair B  |     0.88    | Open
                          Pair C  |     0.90    | Open
                          Pair D  |     0.92    | Open

gi15    |  auto  |        Pair A  |     0.92    | Open
                          Pair B  |     0.88    | Open
                          Pair C  |     0.86    | Open
                          Pair D  |     0.83    | Open

gi16    |  auto  |        Pair A  |     0.92    | Open
                          Pair B  |     0.91    | Open
                          Pair C  |     0.83    | Open
                          Pair D  |     0.83    | Open

gi17    |  auto  |        Pair A  |     0.98    | Open
                          Pair B  |     0.91    | Open
                          Pair C  |     0.85    | Open
                          Pair D  |     0.90    | Open

gi18    |  auto  |        Pair A  |     6.00    | Normal
                          Pair B  |     6.00    | Normal
                          Pair C  |     6.00    | Normal
                          Pair D  |     6.00    | Normal

gi19    |  auto  |        Pair A  |     0.97    | Open
                          Pair B  |     0.93    | Open
                          Pair C  |     0.87    | Open
                          Pair D  |     0.86    | Open

gi20    |  auto  |        Pair A  |     0.95    | Open
                          Pair B  |     0.95    | Open
                          Pair C  |     0.87    | Open
                          Pair D  |     0.91    | Open

gi21    |  auto  |        Pair A  |     0.90    | Open
                          Pair B  |     0.88    | Open
                          Pair C  |     0.83    | Open
                          Pair D  |     0.82    | Open

gi22    |  auto  |        Pair A  |     0.88    | Open
                          Pair B  |     0.87    | Open
                          Pair C  |     0.87    | Open
                          Pair D  |     0.92    | Open

gi23    |  auto  |        Pair A  |     0.91    | Open
                          Pair B  |     0.86    | Open
                          Pair C  |     0.87    | Open
                          Pair D  |     0.83    | Open

gi24    |  auto  |        Pair A  |     0.90    | Open
                          Pair B  |     0.90    | Open
                          Pair C  |     0.88    | Open
```

```
                                Pair D  |     0.88     | Open
```

show fiber-ports optical-transceiver

To show the optical transceiver diagnostics, use the **show fiber-ports optical-transceiver** Privileged EXEC Mode command.

Syntax

show fiber-ports optical-transceiver interfaces *interface-id* **[detailed]**

Parameters

- **interfaces** *interface-id*—Specifies an Ethernet interface ID or a list of Ethernet interface IDs.
- **detailed**—(Optional) Displays the detailed diagnostics.

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show fiber-ports optical-transceiver interfaces gi1-24 detailed
 Port   | Temperature  | Voltage     | Current     | Output power | Input power
| LOS
       | [C]          | [Volt]      | [mA]        | [mWatt]      | [mWatt]     |
================================================================================
=========
  gi1   | Copper
  gi2   | Copper
  gi3   | Copper
  gi4   | Copper
  gi5   | Copper
  gi6   | Copper
  gi7   | Copper
  gi8   | Copper
  gi9   | Copper
 gi10   | Copper
 gi11   | Copper
 gi12   | Copper
 gi13   | Copper
 gi14   | Copper
 gi15   | Copper
 gi16   | Copper
```

```
gi17    | Copper
gi18    | Copper
gi19    | Copper
gi20    | Copper
gi21    | Copper
gi22    | Copper
gi23    | Copper
gi24    | Copper

Temp          - Internally measured transceiver temperature
Voltage       - Internally measured supply voltage
Current       - Measured TX bias current
Output Power - Measured TX output power in milliWatts
Input Power   - Measured RX received power in milliWatts
LOS           - Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

26

Power over Ethernet (PoE) Commands

The Power over Ethernet (PoE) feature is only available on the PoE-based switches.

power inline

To configure the inline power administrative mode on an interface, use the **power inline** Interface Configuration mode command.

Syntax

power inline auto [**time-range** *NAME*]

power inline never

Parameters

- **auto**—Turns on the device discovery protocol and applies power to the device.
- *NAME*—Specify the name of time-range settings. When the time range is not in effect the power is not supplied the attached device. If a time range is not specified, there is no time range bounded to the port. (Range: 1–32 characters.)
- **never**—Turns off the device discovery protocol and stops supplying power to the device.

Default Configuration

The default is **auto**.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example turns on the device discovery protocol on port 1:

```
switch(config)# interface gi1
switch(config-if)# power inline auto

The example shows how to apply workhour time-range to an interface.
Switch(config)# interface gi1
Switch(config-if)# power inline auto time-range workhour

Use the following command to verify your configuration.
Switch(config-if)# do show power inline interface gi1

Port State Status     Priority Class   Max.Power (Admin) Device
                                       (mW)
---- ----- ---------- -------- ------- ----------------- --------
gi1  Auto  off        low      class0  30000 (30000)     N/A

Port Overload Short Current Power Denied MPS Absent Invalid Sig.
---- ------------ ------------ ------------ ------------ ---
gi1  0            0            0            0            0

Port Time Range                        Status
---- --------------------------------- --------
gi1  workhour                          Active
```

power inline legacy enable

To enable supporting legacy powered devices, use the **power inline legacy enable** Global Configuration mode command.

To disable supporting legacy powered devices, use the **no** form of this command.

Syntax

power inline legacy enable

no power inline legacy enable

Default Configuration

Power inline legacy is disabled.

Command Mode

Global Configuration mode

User Guidelines

This feature only works when establishing the autonegotiation connection. For the legacy powered devices that are already connected, disabling this feature only takes effect after you unplug their cables.

Example

```
switchxxxxxx(config)# power inline legacy enable
```

power inline limit

To limit the power consumption on an interface, use the **power inline limit** Interface Configuration mode command.

To revert to its default setting, use the **no** form of the command.

Syntax

power inline limit *power*

no power inline limit

Parameters

- *power*—Maximum amount of power consumption in milliwatts on the interface. (Range: 0 to 30000 milliwatts)

Default Configuration

30000 milliwatts for 802.3at ports and 15400 milliwatts for other ports.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi1
```

```
switchxxxxxx(config-if)# power inline limit 20000
```

power inline limit-mode

To set the power limit mode, use the **power inline limit-mode** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

power inline limit-mode {**class** | **port**}

no power inline limit-mode

Parameters

- **class**—Specifies that the power limit of a port is based on the class of the Power Device (PD) as detected during the classification process.
- **port**—Specifies that the power limit of a port is fixed regardless of the class of the discovered PD.

Command Mode

Global Configuration mode

Example

The following example limits the power per port in class mode:

```
switchxxxxxx(config)# power inline limit-mode class
```

power inline priority

To configure the inline power management priority for an interface, use the **power inline priority** Interface Configuration (Ethernet) mode command.

Syntax

power inline priority {**critical** | **high** | **low**}

Parameters

- **critical**—Specifies that the powered device operation is critical.
- **high**—Specifies that the powered device operation is high priority.
- **low**—Specifies that the powered device operation is low priority.

Default Configuration

The default is **low**.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example sets the inline power management priority for port 4 to high:

```
switchxxxxxx(config)# interface gi4
switchxxxxxx(config-if)# power inline priority high
```

power inline traps enable

To enable inline power traps, use the **power inline traps enable** Global Configuration mode command.

To disable inline power traps, use the **no** form of this command.

Syntax

power inline traps enable

no power inline traps enable

Default Configuration

Inline power traps are disabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# power inline traps enable
```

power inline usage-threshold

To configure the threshold for initiating inline power usage alarms, use the **power inline usage-threshold** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

power inline usage-threshold *percent*

no power inline usage-threshold

Parameters

- *percent*—The usage threshold in percentage of the power limit. An alarm is initiated if the power exceeds this value. (Range: 1 to 99)

Default Configuration

The default threshold is 95 percent.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# power inline usage-threshold 90
```

show env all

To show the environment temperature, the temperature thresholds, and the fan speeds, use the **show env all** Privileged EXEC mode command.

Syntax

show env all

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx(config)# show env all
FAN is OK
TEMPERATURE is OK
```

show power inline

To display information about the inline power for all interfaces or for a specific interface, use the **show power inline** Privileged EXEC mode command.

Syntax

show power inline [*interface-id*]

Parameters

- *interface-id*—Specifies an interface ID. The Interface ID must be an Ethernet port.

Default Configuration

Show information for all ports.

Command Mode

Privileged EXEC mode

Example

Example 1—The following example shows the inline power settings for all interfaces:

```
SwitchXXXXXX# show power inline
Power management mode: Class limit mode
Legacy device support: Disabled
Unit  Power  Status   Nominal     Allocated      Consumed     Available
Usage    Traps
                      Power       Power          Power        Power
Threshold
---- ------- ------ --------- ---------------- ----------- -------------  ---
---   --------
 1     On   Normal 375Watts   15Watts (4%)      5Watts     360Watts     95
Disable

Port    State      Status    Priority  Class  Max. Power (mW)  Alloc. Power
(mW) Device
----- ----------- ---------- -------- ------- ---------------- --------------
--- ------------------------
fa1    Auto       On         Low      Class3  15400            15400
AIR-CAP3502I-T-K9
fa2    Auto       On         Low      Class3  15400            15400
Ieee PD
fa3    Auto       Off        Low      N/A     30000            0
N/A
fa4    Auto       Off        Low      N/A     30000            0
N/A
fa5    Auto       Off        Low      N/A     15400            0
N/A
fa6    Auto       Off        Low      N/A     15400            0
N/A
fa7    Auto       Off        Low      N/A     15400            0
N/A
fa8    Auto       Off        Low      N/A     15400            0
N/A
--More-
```

Example 2—The following example shows the inline power settings for port fa1-2:

```
SwitchXXXXXX# show power inline interfaces fa1-2
Port State Status     Priority Class   Max.Power Alloc.Power Device
                                       (mW)      (mW)
---- ----- ---------- -------- ------- --------- ----------- ----------------
fa1  Auto  searching  low      N/A     30000     0           N/A
fa2  Auto  on         low      class3  15400     15400       Ieee PD

Port Overload      Short Current  Power Denied  MPS Absent    Invalid Sig.
---- ------------- -------------- ------------- ------------- -------------
```

```
fa1  0             0             0             0             0
fa2  0             0             0             0             0

Port Time Range                          State
---- ----------------------------------- --------
fa1
fa2  TimebasedPoE                        Active
```

show power inline consumption

To show the inline power consumption for all interfaces or for a specific interface, use the **show power inline consumption** Privileged EXEC mode command.

Syntax

show power inline consumption [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface must be an Ethernet port.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the inline power consumption for port 1:

```
switchxxxxxx# show power inline consumption interfaces gi1
Port Max.Power (Admin)  Power    Voltage  Current
       (mW)                (mW)      (mV)      (mA)
---- ----------------- -------- -------- --------
gi1  30000 (30000)        0         0         0
```

The following table describes the significant fields shown in the example:

Field	Description
Port	Interface number.

Max. Power (Admin)	Maximum amount of power in milliwatts allocated to the selected interface.
Power	Amount of power in milliwatts assigned to the powered device connected to the selected interface.
Voltage	Voltage of the power.
Current	Current in milliampere of the power.

27

Port Channel Commands

channel-group

To associate a port with a port channel, use the **channel-group** Interface Configuration mode command.

To remove a port from a port channel, use the **no** form of this command.

Syntax

channel-group *port channel* **mode** {**active** | **on** | **passive**}

no channel-group

Parameters

- *port channel*—The number of the port channel that the port will join.
- **mode**—Specifies the mode of the port channel. The possible values are:
  - **active**—Enables LACP unconditionally. It forces unconditionally the port to join a channel as a result of a LACP operation.
  - **on**—Enables static only. It forces the port to join a channel without a LACP operation. In this mode, a usable EtherChannel exists only when both connected port groups are in the on mode.
  - **passive**—Enables LACP only if a LACP device is detected. It forces the port to join a channel as a result of a LACP operation. Active mode places a port into a negotiating state in which the port initiates the negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

Default Configuration

The port is not assigned to a port channel.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example forces gi1 to join the port channel 1 without a LACP operation:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# channel-group 1 mode on
```

port-channel load-balance

To configure the load-balancing policy for a port channel, use the **port-channel load-balance** Global Configuration mode command.

Syntax

port-channel load-balance {**src-dst-mac** | **src-dst-mac-ip**}

Parameters

- **src-dst-mac**—Specifies that the port channel load-balancing is based on the source and destination MAC addresses for all packets.
- **src-dst-mac-ip**—Specifies that the port channel load-balancing is based on the destination IP addresses, source IP addresses, destination MAC addresses, and source MAC addresses for all packets.

Default Configuration

The default option is **src-dst-mac**.

Command Mode

Global Configuration mode

User Guidelines

In the **src-dst-mac-ip** port channel load-balancing policy, fragmented packets may be reordered.

Example

```
switchxxxxxx(config)# port-channel load-balance src-dst-mac
```

show etherchannel summary

To show information for all port channels, use the **show etherchannel summary** Privileged EXEC Mode command.

Syntax

show etherchannel summary

Parameters

N/A

Command Mode

Privileged EXEC Mode

Examples

```
switchxxxxxx# show etherchannel summary
Load Balancing: src-dst-mac.

Flags: D - down
           P - bundled in port-channel
           H - Hot-standby (LACP only)
           U - in use
           w - waiting to be aggregated

Number of channel-groups in use: 4

Group Port-channel Protocol Ports
--------+---------------+---------+-------------------------------------
1         po1(U)           ---         fa4(P) fa5(D) fa19(D) fa20(D)
                                              fa21(D) fa22(D)
2         po2(D)           LACP   fa7(D)  fa8(D)
3         po3(D)           ---         fa15(D) fa16(D) fa17(D)
4         po4(U)           ---         fa9(D) fa10(D) fa18(D) fa23(P)
                                             fa24(P)
```

28

Port Monitor Commands

monitor session destination interface

To start a destination interface (monitoring) of a port monitor session (mirroring), use the **monitor session destination interface** Global Configuration mode command.

To stop a destination interface of a port monitoring session, use the **no** form of this command.

Syntax

monitor session *session-number* **destination interface** *interface-id* [**allow-ingress-packet**]

no monitor session *session-number* **destination interface** *interface-id*

Parameters

- *session-number*—The identifier for a port monitor session. (Range: 1 to 4)
- *interface-id*—The destination interface ID. The interface must be an Ethernet interface.
- **allow-ingress-packet**—(Optional) Enables ingress traffic forwarding for the destination interface.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

This command specifies the destination port for a monitor session. The following restrictions apply to the ports that are configured to be monitored ports:

- The port cannot be source port.
- The port is not a member in the port channel.
- GVRP is not enabled on the port.

Example

The following example defines the destination port fa24 for the monitor session 1:

```
switchxxxxxx(config)# monitor session 1 destination interface gi24
```

monitor session destination remote-span

To start a destination interface for remote SPAN, use the **monitor session destination remote-span** Global Configuration mode command.

To stop a destination interface for remote SPAN, use the **no** form of this command.

Syntax

monitor session *session-number* **destination remote-span vlan** *vlan-id* **reflector-interface** *interface-id*

no monitor session *session-number* **destination remote-span**

Parameters

- *session-number*—The identifier of the monitor session. (Range: 1 to 4)
- **vlan** *vlan-id*—Specifies the remote VLAN for a RSPAN destination session. (Range: 2 to 4094)
- **reflector-interface** *interface-id*—Specifies the reflector interface ID. The interface ID must be an Ethernet port.

Command Mode

Global Configuration mode

Example

The following example defines the destination remote-span VLAN 2 and reflector interface fa11 for the monitor session 1:

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 destination remote-span vlan 2
reflector-interface gi11
```

monitor session source interfaces

To start a source interface (monitored) of a port monitor session (mirroring), use the **monitor session source interfaces** Global Configuration mode command.

Use the **no** form of this command to stop a port monitor session.

Syntax

monitor session *session-number* **source interfaces** *interface-id* {**both** | **rx** | **tx**}

no monitor session *session-number* **source interfaces** *interface-id* {**both** | **rx** | **tx**}

monitor session *session-number* **source vlan** *vlan-id*

no monitor session *session-number* **source vlan**

Parameters

- *session-number*—The identifier for the port monitor session. (Range: 1 to 4)
- *interface-id*—The source interface ID. The interface ID must be an Ethernet port.
- **both**—Monitors both transmitted and received packets.
- **rx**—Monitors received packets only.
- **tx**—Monitors transmitted packets only.
- **vlan** *vlan-id*—Specifies a VLAN.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

This command specifies the source ports for a monitor session. The port that is configured to be a source port cannot be a destination port.

NOTE In this mode some traffic duplication on the analyzer port may be observed. For example:

- Port 2 is being egress monitored by port 4.
- Port 2 and 4 are members in VLAN 3.
- Unknown unicast packet sent to VLAN 3 will egress from port 4 twice, one instance as normal forward and another instance as mirrored from port 2.
- Moreover, if port 2 is an untagged member in VLAN 3 and port 4 is a tagged member, then both instances will look different (one tagged and the other is not).

Example

The following example copies traffic for both directions (Tx and Rx) from the source port fa2 to the monitor session 1:

```
switchxxxxxx(config)# monitor session 1 source interfaces gi2 both
```

monitor session source remote-span

To start a source interface for remote SPAN (RSPAN), use the **monitor session source remote-span** Global Configuration mode command.

To stop a source interface for remote SPAN, use the **no** form of this command.

Syntax

monitor session *session-number* **source remote-span vlan** *vlan-id*

no monitor session *session-number* **source remote-span**

Parameters

- *session-number*—RSPAN monitor session number. (Range: 1 to 4)
- **vlan** *vlan-id*—Specifies the remote VLAN for a RSPAN source session. The VLAN is used to copy traffic to another device. (Range: 2 to 4094)

Command Mode

Global Configuration mode

Example

The following example defines the source remote-span VLAN 2 for the monitor session 1:

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote-span vlan 2
```

no monitor session

To disable all monitor sessions or disable a specific monitor session, use the **no monitor session** Global Configuration mode command.

Syntax

no monitor session {*session number* | **all** | **local** | **remote**}

Parameters

- *session number*—A specific monitor session to be disabled. (Range: 1 to 4)
- **all**—Disables all monitor sessions.
- **local**—Disables a local monitor session.
- **remote**—Disables a RSPAN session.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# no monitor session all
```

remote-span

To enable remote SPAN, use the **remote-span** VLAN Configuration mode command.

To disable remote SPAN, use the **no** form of this command.

Syntax

remote-span

no remote-span

Parameters

N/A

Command Mode

VLAN Configuration mode

Example

The following example defines VLAN 2 as a RSPAN VLAN:

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
```

show monitor

To show the status for all monitor sessions or for a specific monitor session, use the **show monitor** Privileged EXEC Mode command.

Syntax

show monitor [**session** *session-number*]

Parameters

- **session** *session-number*—(Optional) Specifies the identifier of the monitor session. If not specified, all monitor sessions will be displayed. (Range: 1 to 4)

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show monitor

Session 1 Configuration
Session Type  : Unknown
Mirrored source   : Not Config
Destination port  : Not Config


Session 2 Configuration
Session Type  : Unknown
Mirrored source   : Not Config
Destination port  : Not Config


Session 3 Configuration
Session Type  : Unknown
Mirrored source   : Not Config
Destination port  : Not Config


Session 4 Configuration
Session Type  : Unknown
Mirrored source   : Not Config
Destination port  : Not Config
```

show vlan remote-span

To show the remote SPAN VLAN, use the **show vlan remote-span** Privileged EXEC Mode command.

Syntax

show vlan remote-span

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show vlan remote-span
Remote SPAN VLAN ID: 3
```

29

QoS Commands

class

To attach an access control list (ACL) to a policy map, use the **class** Policy-map Configuration mode command.

To detach a class map from a policy map, use the **no** form of this command.

NOTE This command is available only when the switch is in quality of service (QoS) advanced mode.

Syntax

class *class-map-name*

no class *class-map-name*

Parameters

- *class-map-name*—Enter the name for an existing class map. If the class map does not exist, a new class map is created under the specified name.

Default Configuration

No class map is defined for the policy map.

Command Mode

Policy-map Configuration mode

User Guidelines

This command is the same as creating a class map and then binding it to the policy map. After the policy map is defined, use the **service-policy** command to attach it to a port or port channel.

Example

The following example defines a traffic classification (class map) called class1 containing an ACL called enterprise. The class is in a policy map called policy1. The policy-map policy1 now contains the ACL enterprise.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
```

class-map

To create or modify a class map and enter the Class-Map Configuration mode, use the **class-map** Global Configuration mode command and its subcommands.

To delete a class map, use the **no** form of this command.

NOTE All class map commands are available only when the switch is in QoS advanced mode.

Syntax

class-map *class-map-name* [**match-any**]

no class-map *class-map-name*

Parameters

- *class-map-name*—The class map name.
- **match-any**—(Optional) Performs a logical OR of the criteria of ACLs belonging to this class map. Only a single match criteria in this class map must be matched.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

A class map consists of one or more ACLs. It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

The **class-map** command enters the Class-map Configuration mode. In this mode, up to two **match** commands can be entered to configure the criteria for this class. Each **match** specifies an ACL.

When using two **match** commands, each must point to a different type of ACL, such as one IP-based ACL and one MAC-based ACL. The classification is by first matching, therefore, the order of the ACLs is important.

Error messages are generated in the following cases:

- There is more than one **match** command in a **match-all** class map.
- There is a repetitive classification field in the participating ACLs.

After entering the Class-map Configuration mode, the following configuration commands are available:

- **do**—Run the EXEC commands in the Class-map Configuration mode.
- **end**—End the current mode and return to the Privileged EXEC mode.
- **exit**—Exit the Class-map Configuration mode and return to the Global Configuration mode.
- **match**—Configure the match criteria to classify traffic.
- **no**—Remove a match statement from a class map.

Example

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the ACL specified:

```
switchxxxxxx(config)# class-map class1 match-any
switchxxxxxx(config-cmap)# match access-group acl-name
```

match

To bind an ACL to the class map being configured, use the **match** Class-map Configuration mode command.

To delete the match criteria, use the **no** form of this command.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

Parameters

- **access-group** *acl-name*—Specifies the name of a MAC-based ACL, IPv4-based ACL, or IPv6-based ACL.

Default Configuration

No match criterion is supported.

Command Mode

Class-Map Configuration mode

Example

The following example defines a class map called Class1. Class1 contains an ACL called enterprise. Only traffic matching all criteria in enterprise belongs to the class map.

```
switchxxxxxx(config)# class-map class1
switchxxxxxx(config-cmap)# match access-group enterprise
```

police

To define a policer for classified traffic, use the **police** Policy-map Class Configuration mode command. This command defines another group of actions for the policy map (per class map).

To remove a policer, use the **no** form of this command.

This command is used after the **policy-map** and **class** commands.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

police *committed-rate-kbps* [**exceed-action** {**drop** | **forward**}]

no police

Parameters

- *committed-rate-kbps*—The average traffic rate (CIR) in kbits per second (kbps). (Range: 16 to 10000000)
- **exceed-action** {**drop** | **forward**}—(Optional) Specifies the action to be taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **forward**—Forwards the packet.

Default Usage

N/A

Command Mode

Policy-map Class Configuration mode

User Guidelines

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket.

Example

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps, the packet is dropped. The class is called class1 and is in a policy map called policy1.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police 124000 exceed-action drop
```

police aggregate

To apply an aggregate policer to multiple class maps within the same policy map, use the **police aggregate** Policy-map Class Configuration mode command.

To remove an existing aggregate policer from a policy map, use the **no** form of this command.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate

Parameters

- *aggregate-policer-name*—The aggregate policer name.

Command Mode

Policy-map Class Configuration mode

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the **exit** command to return to the Global Configuration mode. Use the **end** command to return to the Privileged EXEC mode.

Example

The following example applies the aggregate policer called Policer1 to a class called class1 in a policy map called policy1 and class2 in policy map policy2:

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 exceed-action
drop
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police aggregate policer1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)# policy-map policy2
switchxxxxxx(config-pmap)# class class2
switchxxxxxx(config-pmap-c)# police aggregate policer1
```

policy-map

To create a policy map and enter the Policy-map Configuration mode, use the **policy-map** Global Configuration mode command.

To delete a policy map, use the **no** form of this command.

NOTE This command is only available when the switch is in QoS advanced mode.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters

- *policy-map-name*—The policy map name. (Range: 0 to 32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

A policy map contains one or more class maps and an action that is taken if the packet matches the class map. Policy maps may be bound to ports or port channels.

Use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

Entering the Policy-map Global Configuration mode also enables configuring or modifying the class policies for that policy map. Class policies in a policy map can be configured only if the classes have match criteria defined for them.

Policy map is applied on the ingress path.

The match criteria is for a class map. Only one policy map per interface is supported. The same policy map can be applied to multiple interfaces and directions.

The **service-policy** command binds a policy map to a port or a port channel.

Example

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode:

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)#
```

priority-queue out num-of-queues

To set the number of expedite queues, use the **priority-queue out num-of-queues** Global Configuration mode command.

Syntax

priority-queue out num-of-queues *number-of-queues*

Parameters

- *number-of-queues*—The number of queues to be expedite (SP) queues. The expedite queues would be the queues with the higher indexes. (Range: 0 to 8)

  There must be either 0 WRR queues or more than one. If the *number-of-queues* is set to 0, all queues are assured forwarding (according to the WRR weights). If the *number-of-queues* is set to 8, all queues are expedited (SP queues).

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

An expedite queue is a Strict Priority (SP) queue, which is serviced until empty before the other lower priority queues are serviced.

The weighted round robin (WRR) weight ratios are affected by the number of expedited queues, because there are fewer queues participating in WRR. This indicates that the corresponding weight in the **wrr-queue bandwidth** Interface Configuration mode command is ignored (not used in the ratio calculation).

Example

The following example configures the number of expedite queues as 2:

```
switchxxxxxx(config)# priority-queue out num-of-queues 2
```

qos

To enable QoS on the switch and set its operation mode, use the **qos** Global Configuration mode command.

To disable QoS on the switch, use the **no** form of this command.

Syntax

qos [**basic** | **advanced** [**ports-not-trusted** | **ports-trusted**]]

no qos

Parameters

- **basic**—(Optional) Enables QoS basic mode. If no option is specified, the QoS mode is set to the basic mode by default.
- **advanced**—(Optional) Enables QoS advanced mode, which enables the full range of QoS configuration.
- **ports-not-trusted**—(Optional and relevant for advanced mode only) Indicates that the packets, which are not classified by policy map rules to a QoS action, are mapped to egress queue 0. This is the default setting in advanced mode.
- **ports-trusted**—(Optional and relevant for advanced mode only) Indicates that the packets, which are not classified by policy map rules to a QoS action, are mapped to an egress queue based on the packet's fields. Use the **qos advanced-mode trust** command to specify the trust mode.

Default Configuration

If **qos** is entered without any keywords, the QoS basic mode is enabled.

If **qos advanced** is entered without a keyword, the default is **ports-not-trusted**.

Command Mode

Global Configuration mode

Examples

Example 1—The following example enables QoS basic mode on the switch:

```
switchxxxxxx(config)# qos basic
```

Example 2—The following example enables QoS advanced mode on the switch with the **ports-not-trusted** option:

```
switchxxxxxx(config)# qos advanced
This action will cause loss of configuration.Proceed?(y)   (Y/N)[Y]
```

qos advanced-mode trust

To configure the trust mode in QoS advanced mode, use the **qos advanced-mode trust** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

qos advanced-mode trust {**cos** | **cos-dscp** | **dscp** | **ip-precedence**}

no qos advanced-mode trust

Parameters

- **cos**—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- **cos-dscp**—Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.
- **dscp**—Classifies ingress packets with the packet DSCP values.
- **ip-precedence**—Classifies ingress packets with the packet precedence values.

Default Configuration

The default trust mode is **cos**.

Command Mode

Global Configuration mode

User Guidelines

The configuration is relevant for QoS advanced mode in the following cases:

- **ports-not-trusted mode**—For packets that are classified to the QoS action trust.
- **ports-trusted mode**—For packets that are not classified to any QoS action or classified to the QoS action trust.

Example

The following example sets CoS as the trust mode in QoS advanced mode:

```
switchxxxxxx(config)# qos advanced-mode trust cos
```

qos aggregate-policer

To define the policer parameters that can be applied to multiple traffic classes within the same policy map, use the **qos aggregate-policer** Global Configuration mode command.

To remove an existing aggregate policer, use the **no** form of this command.

NOTE This command is only available when the switch is in QoS advanced mode.

Syntax

qos aggregate-policer *name committed-rate-kbps* [**exceed-action** {**drop** | **forward**}]

no qos aggregate-policer *name*

Parameters

- *name*—The aggregate policer name.
- *committed-rate-kbps*—The average traffic rate (CIR) in kbits per second (kbps). (Range: 16 to 1000000)
- **exceed-action** {**drop** | **forward**}—(Optional) Specifies the action to be taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **forward**—Forwards the packet.

Default Configuration

No aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

Define an aggregate policer if the policer aggregates traffic from multiple class maps.

Aggregate policers cannot aggregate traffic from multiple devices. If the aggregate policer is applied to more than one device, traffic on each device is counted separately and is limited per device.

Traffic from two different ports on the same device can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration mode command must first be used to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

Example

The following example defines the parameters of a policer called Policer1 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer test1 124000 exceed-action drop
```

qos cos

To define the default CoS value for an interface, use the **qos cos** Interface Configuration mode command.

Syntax

qos cos *default-cos*

Parameters

- *default-cos*—The default CoS value (VPT value) of the interface. If the interface is trusted and the packet is untagged, then the default CoS value becomes the CoS value. (Range: 0 to 7)

Default Configuration

The default CoS value of an interface is 0.

Command Mode

Interface Configuration mode

User Guidelines

Use the default CoS value to assign a CoS value to all untagged packets entering the interface.

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# qos cos 5
```

qos map cos-queue

To map assigned CoS values to an egress queue, use the **qos map cos-queue** Global Configuration mode command.

Syntax

qos map cos-queue *cos0...cos7* **to** *queue-id*

Parameters

- *cos0... cos7*—Up to eight CoS values to map to the specified queue number. (Range: 0 to 7)
- **to** *queue-id*—Specifies the queue number to which the CoS values are mapped.

Default Configuration

CoS-to-Queue mapping matrix

COS	0	1	2	3	4	5	6	7
Queue	2	1	3	4	5	6	7	8

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# qos map cos-queue 2 to 7
```

qos map dscp-queue

To configure the DSCP-to-CoS map, use the **qos map dscp-queue** Global Configuration mode command.

Syntax

qos map dscp-queue *dscp-list* **to** *queue-id*

Parameters

- *dscp-list*—Up to eight DSCP values, separated by spaces to map to the specified queue number. (Range: 0 to 63)
- **to** *queue-id*—Specifies the queue number to which the DSCP values are mapped.

Default Configuration

DSCP-to-Queue mapping matrix

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Queue	1	2	3	4	5	6	7	8

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# qos map dscp-queue 3 to 6
```

qos map precedence-queue

To configure the IP precedence-to-queue map, use the **qos map precedence-queue** Global Configuration mode command.

Syntax

qos map precedence-queue *ip-precedence-list* **to** *queue-id*

Parameters

- *ip-precedence-list*—Up to eight IP precedence values, separated by spaces, to map to the specified queue number. (Range: 0 to 7)
- **to** *queue-id*—Specifies the queue number to which the IP precedence values are mapped.

Default Configuration

IP precedence-to-queue mapping matrix

IP Precedence	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# qos map precedence-queue 2 to 7
```

qos map queue-cos

To configure the queue-to-CoS map, use the **qos map queue-cos** Global Configuration mode command.

Syntax

qos map queue-cos *queue-list* **to** *cos-id*

Parameters

- *queue-list*—Up to eight queue numbers to map to the specified CoS value. (Range:1 to 8)
- **to** *cos-id* —Specifies the CoS value to which the queue values are mapped.

Default Configuration

Queue-to-CoS mapping matrix

Queue	1	2	3	4	5	6	7	8
COS	1	0	2	3	4	5	6	7

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# qos map queue-cos 7 to 2
```

qos map queue-dscp

To configure the queue-to-DSCP map, use the **qos map queue-dscp** Global Configuration mode command.

Syntax

qos map queue-dscp *queue-list* **to** *dscp-id*

Parameters

- *queue-list*—Up to eight queue numbers to map to the specified DSCP values. (Range:1 to 8)
- **to** *dscp-id* —Specifies the DSCP values to which the queue values are mapped.

Default Configuration

Queue-to-DSCP mapping matrix

Queue	1	2	3	4	5	6	7	8
DSCP	0-7	8-16	16-23	24-31	32-39	40-47	48-55	56-63

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# qos map queue-dscp 7 to 50
```

qos map queue-precedence

To configure the queue-to-precedence map, use the **qos map queue-precedence** Global Configuration mode command.

Syntax

qos map queue-precedence *queue-list* **to** *ip-precedence-id*

Parameters

- *queue-list*—Up to eight queue numbers to map to the specified IP precedence value. (Range:1 to 8)
- **to** *ip-precedence-id* —Specifies the precedence value to which the queue values are mapped.

Default Configuration

Queue-to-precedence mapping matrix

Queue	1	2	3	4	5	6	7	8
IP Precedence	0	1	2	3	4	5	6	7

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# qos map queue-precedence 8 to 7
```

qos remark

To configure the remarking state of each interface, use the **qos remark** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

qos remark {**cos** | **dscp** | **ip-precedence**}

no qos remark {**cos** | **dscp** | **ip-precedence**}

Parameters

- **cos**—Remarks the ingress packets with the CoS value.
- **dscp**—Remarks the ingress packets with the DSCP value.
- **ip-precedence**—Remarks the ingress packets with the IP precedence value.

Default Configuration

No any remarking is defined.

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi10
switchxxxxxx(config-if)# qos remark dscp
```

qos trust (Global)

To configure the trust state for QoS basic mode, use the **qos trust** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

NOTE This command is available only when the switch is in QoS basic mode.

Syntax

qos trust {**cos** | **cos-dscp** | **dscp** | **ip-precedence**}

no qos trust

Parameters

- **cos**—Classifies the ingress packets with packet CoS value. Untagged packets are classified with the default port CoS value.
- **cos-dscp**—Classifies the ingress packets with packet CoS-DSCP value.
- **dscp**—Classifies the ingress packets with packet DSCP value.
- **ip-precedence**—Classifies the ingress packets with packet IP precedence value.

Default Configuration

The default trust mode is **dscp**.

Command Mode

Global Configuration mode

User Guidelines

Packets entering a QoS domain are classified at its edge. 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.

When the switch is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-to-queue map.

When the switch is configured with trust CoS, the traffic is mapped to the queue by the CoS-to-queue map.

Example

```
switchxxxxxx(config)# qos trust cos
```

qos trust (Interface)

To enable the trust state on an interface when the switch is in QoS basic mode, use the **qos trust** Interface Configuration mode command.

To disable the trust state on an interface, use the **no** form of this command.

Syntax

qos trust

no qos trust

Parameters

N/A

Default Configuration

Trust state is enabled on each interface when the switch is in QoS basic mode.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# qos trust
```

service-policy

To bind a policy map to a port or port channel, use the **service-policy** Interface Configuration mode command.

To detach a policy map from an interface, use the **no** form of this command.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

service-policy input *policy-map-name*

no service-policy input

Parameters

- **input** *policy-map-name*—Specifies the policy map to apply to the input interface.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

Only one policy map per interface per direction is supported.

Example

The following example attaches a policy map called Policy1 to the input interface:

```
switchxxxxxx(config-if)# interface gi11
switchxxxxxx(config-if)# service-policy input policy1
```

set

To select the value that QoS uses as the DSCP value, the egress queue, or to set user priority values, use the **set** Policy-map Class Configuration mode command.

To revert to its default setting, use the **no** form of this command.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

set queue *queue-id*

no set queue

Parameters

- **queue** *queue-id*—Specifies the egress queue. (Range: 1 to 8)

Command Mode

Policy-map Class Configuration mode

User Guidelines

The **set** and **trust** commands are mutually exclusive within the same policy map.

To return to the Global Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map, and sets the DSCP value in the packet to 56 for classes in the policy map called p1:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-mac-al)# permit ip any any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# set queue 2
```

show class-map

To show information for all class maps or for a specific class map when the switch is in QoS advanced mode, use the **show class-map** Privileged EXEC mode command.

Syntax

show class-map [*class-map-name*]

Parameters

- *class-map-name*—(Optional) The class map name.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show class-map class1
Class Map match-any class1 (id4)
Match IP dscp 11 21
```

show policy-map

To show information for all policy maps or for a specific policy map, use the **show policy-map** Privileged EXEC mode command.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

show policy-map [*policy-map-name*]

Parameters

- *policy-map-name*—(Optional) The policy map name.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show policy-map
Policy Map policy1
class class1
set IP dscp 7
Policy Map policy2
class class 2
police 96000 exceed-action drop
class class3
police 124000 exceed-action policed-dscp-transmit
```

show policy-map interface

To show the policy map that is applied to an interface, use the **show policy-map interface** Privileged EXEC mode command.

Syntax

show policy-map interface *interface-id*

Parameters

- *interface-id*—An interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show policy-map interface fa5
Interface         Input Policy
---------         -------------
fa5               pmap1
```

show qos

To show the QoS settings on the switch, use the **show qos** Privileged EXEC mode command.

Syntax

show qos

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays QoS attributes when the switch is in QoS basic mode:

```
switchxxxxxx# show qos
Basic trust: dscp
Qos: basic
```

Example 2—The following example displays QoS attributes when the switch is in QoS advanced mode:

```
switchxxxxxx# show qos
QoS Mode: advanced
Advanced mode trust type: cos
Advanced mode ports state: Not trusted
```

show qos aggregate-policer

To show information for specific aggregate policers, use the **show qos aggregate-policer** Privileged EXEC mode command.

NOTE This command is available only when the switch is in QoS advanced mode.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

Parameters

- *aggregate-policer-name*—(Optional) The aggregate policer name.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show qos aggregate-policer policer1
aggregate-policer policer1 96000 exceed-action drop
```

show qos interfaces

To show the QoS configuration on all interfaces or on an interface, use the **show qos interfaces** Privileged EXEC mode command.

Syntax

show qos interfaces *interface-id*

Parameters

- *interface-id*—An interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

If a specific interface is not specified, information for all interfaces is displayed.

Example

```
switchxxxxxx# show qos interface gi1
Port|CoS|Trust State|Remark Cos|Remark DSCP|Remark IP Prec
----+---+-----------+----------+-----------+----------------
gi1 | 0 |  enabled   | disabled |  disabled |    disabled
```

show qos map

To show information for various types of QoS mapping, use the **show qos map** Privileged EXEC mode command.

Syntax

show qos map [{**cos-queue** | **dscp-queue** | **ip-precedence-queue** | **queue-cos** | **queue-dscp** | **queue-precedence**}]

Parameters

- **cos-queue**—(Optional) Displays the CoS-to-queue mapping.
- **dscp-queue**—(Optional) Displays the DSCP-to-queue mapping.
- **ip-precedence-queue**—(Optional) Displays the IP precedence-to-queue mapping.
- **queue-cos**—(Optional) Displays the queue-to-CoS mapping.
- **queue-dscp**—(Optional) Displays the queue-to-DSCP mapping.
- **queue-precedence**—(Optional) Displays the queue-to-precedence mapping.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show qos map
CoS to Queue mappings
   COS    0  1  2  3  4  5  6  7
--------------------------------
 Queue    2  1  3  4  5  6  7  8

DSCP to Queue mappings
d1: d2   0  1  2  3  4  5  6  7  8  9
---------------------------------------
 0:      1  1  1  1  1  1  1  2  2  2
 1:      2  2  2  2  2  2  3  3  3  3
 2:      3  3  3  3  4  4  4  4  4  4
 3:      4  4  5  5  5  5  5  5  5  5
 4:      6  6  6  6  6  6  6  6  7  7
 5:      7  7  7  7  7  7  8  8  8  8
 6:      8  8  8  8

IP Precedence to Queue mappings
 IP Precedence   0  1  2  3  4  5  6  7
-----------------------------------------
         Queue     2  1  3  4  5  6  7  8

Queue to CoS mappings
 Queue    1  2  3  4  5  6  7  8
--------------------------------
   CoS    1  0  2  3  4  5  6  7

Queue to DSCP mappings
 Queue    1  2  3  4  5  6  7  8
--------------------------------
  DSCP    0  8 16 24 32 40 48 56

Queue to IP Precedence mappings
 Queue    1  2  3  4  5  6  7  8
--------------------------------
ipprec    0  1  2  3  4  5  6  7
```

show qos queueing

To show the QoS queuing information, use the **show qos queueing** Privileged EXEC mode command.

Syntax

show qos queueing

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show qos queueing
qid-weights    Ef - Priority
1 - N/A         ena- 1
2 - N/A         ena- 2
3 - N/A         ena- 3
4 - N/A         ena- 4
5 - N/A         ena- 5
6 - N/A         ena- 6
7 - N/A         ena- 7
8 - N/A         ena- 8
```

show rate-limit vlan

To show the port rate limit for a specific VLAN or for all VLANs, use the **show rate-limit vlan** Privileged EXEC mode command.

Syntax

show rate-limit vlan *vlan-id*

Parameters

- *vlan-id*—The VLAN ID.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show rate-limit vlan 1
VLAN   |   Port   | rate-limit [Kbps]
--------+--------+-------------------
     1   |  ANY    |          N/A      |
```

traffic-shape

To configure the maximum permitted excess burst size of egress port and queue shaper, use the **traffic-shape** Interface Configuration mode command.

To disable the shaper, use the **no** form of this command.

Syntax

traffic-shape burst [*queue*] *committed-burst*

no traffic-shape

Parameters

- *queue*—(Optional) The queue number to which the shaper is assigned.
- *committed-burst*—The maximum permitted excess burst size (CBS) in bytes. (Range: 128 to 56319 bytes)

Default Configuration

The default shaper burst is 768 bytes.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example sets a traffic shaper burst size 9600 bytes:

```
switchxxxxxx(config)# traffic-shape burst 9600
```

```
switchxxxxxx(config)# traffic-shape burst queue 9600
```

trust-shape (Interface)

To configure the egress port shaper, use **trust-shape** Interface Configuration mode command. The egress port shaper controls the traffic transmit rate (Tx rate).

To disable the shaper, use the **no** form of this command.

Syntax

traffic-shape *committed-rate*

no traffic-shape

Parameters

- *committed-rate*—The maximum average traffic rate in 16 kbits per second (kbps). (Range: 16 to 1000000 kbps)

Default Configuration

The shaper is disabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example sets a traffic shaper on fa5 when the average traffic rate exceeds 124000 kbps:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# traffic-shape 124000
```

traffic-shape queue

To configure the egress queue shaper on a specific queue, use the **traffic-shape queue** Interface Configuration mode command. The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on an interface.

To disable the shaper, use the **no** form of this command.

Syntax

traffic-shape queue *queue-id committed-rate*

no traffic-shape queue *queue-id*

Parameters

- *queue-id*—The queue number to which the shaper is assigned. (Range: 1 to 8)
- *committed-rate*—The average traffic rate in 16 kbits per second (kbps). (Range: 16 to 1000000)

Default Configuration

The shaper is disabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example sets a shaper on queue 1 when the average traffic rate exceeds 124000 kbps:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# traffic-shape queue 1 124000
```

trust

To configure the trust state, use the **trust** Policy-map Class Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

trust

no trust

Parameters

N/A

Default Configuration

The default state is according to the mode selected in the **qos** command (advanced mode). The type of trust is determined in **qos advanced-mode trust**.

Command Mode

Policy-map Class Configuration mode

User Guidelines

This command is relevant only when the switch is in QoS advanced, ports-not-trusted mode. Trust indicates that traffic is sent to the queue according to the packet's QoS parameters (UP or DSCP).

Use this command to distinguish the QoS trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in incoming traffic.

The type of trust is determined in the **qos advanced-mode trust** command.

Trust values set with this command supersede trust values set on specific interfaces with the **qos trust (Interface)** Interface Configuration mode command.

The **trust** and **set** commands are mutually exclusive within the same policy map.

Policy maps, which contain **set** or **trust** commands or that have ACL classification to an egress interface, cannot be attached by using the **service-policy** Interface Configuration mode command.

If specifying trust CoS, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map, and configures the trust state using the DSCP value in the ingress packet:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-mac-al)# permit ip any any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# trust
```

rate-limit (Interface)

To limit the incoming traffic rate on an interface, use the **rate-limit** Interface Configuration mode command.

To disable the rate limit on an interface, use the **no** form of this command.

Syntax

rate-limit *committed-rate-kbps*

no rate-limit

Parameters

- *committed-rate-kbps*—The maximum ingress traffic on an Ethernet interface in kilobits per second (kbps). (Range: 16 to 1000000)

Default Configuration

Rate limiting is disabled.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example limits the incoming traffic rate on fa5 to 100000 kbps:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# rate-limit 100000
```

rate-limit (VLAN)

To limit the incoming traffic rate for a VLAN, use the **rate-limit VLAN** Global Configuration mode command.

To disable the rate limit for a VLAN, use the **no** form of this command.

Syntax

rate-limit *committed-rate* **vlan** *vlan-id*

no rate-limit vlan *vlan-id*

Parameters

- *committed-rate*—The average traffic rate (CIR) in kbps. (Range: 16 to 1000000)
- **vlan** *vlan-id*—Specifies the VLAN ID.

Default Configuration

Rate limiting is disabled.

Command Mode

Global Configuration mode

User Guidelines

Traffic policing in a policy map takes precedence over the VLAN rate limiting. If a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet is counted only in the traffic policing of the policy map.

Example

The following example limits the rate on VLAN 11 to 100000 kbps:

```
switchxxxxxx(config)# rate-limit 100000 vlan 11
```

wrr-queue bandwidth

To assign WRR weights to egress queues, use the **wrr-queue bandwidth** Global Configuration command.

Syntax

wrr-queue bandwidth *weight1 weight2... weightN*

Parameters

- *weight1 weight1... weightN*—The ratio of bandwidth assigned by the WRR packet scheduler to the packet queues. Separate each value by a space. (Range for each weight: 1 to 127)

Default Configuration

WRR is disabled by default. The default WRR weight is 1 for all queues.

Command Mode

Global Configuration mode

User Guidelines

The weight ratio determines the frequency at which the packet scheduler removes packets from each queue.

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. We do not recommend that you set the weight of a queue to 0 as it might stop transmission of control-protocols packets generated by the device.

All three queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

An expedite (SP) queue is a priority queue, which is serviced until empty before the other queues are serviced. The expedite queues are designated by the **priority-queue out num-of-queues** command.

Example

```
switchxxxxxx(config)# priority-queue out num-of-queues 4
switchxxxxxx(config)# wrr-queue bandwidth 6 6 6 6
```

30

RADIUS Commands

radius-server default-param

To set the default Remote Authentication Dial-In User Service (RADIUS) server parameters, use the **radius-server default-param** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

radius-server default-param [**key** *RADIUSKEY*] [**retransmit** *retries*] [**timeout** *timeout*]

no radius-server default-param

Parameters

- **key** *RADIUSKEY*—(Optional) Specifies the key string used for authenticating and encrypting the RADIUS attributes communicated between the switch and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0 to 128 characters)
- **retransmit** *retries*—(Optional) Specifies the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred. (Range: 1 to 10)
- **timeout** *timeout*—(Optional) Specifies the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. (Range: 1 to 30, default: 3)

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# radius-server default-param retransmit 5 timeout 20
```

radius-server host

To configure a RADIUS server, use the **radius-server host** Global Configuration mode command.

To delete a RADIUS server, use the **no** form of the command.

Syntax

radius-server host {*ip-address* | *hostname*} [**acct-port** *acct-port-number*] [**auth-port** *auth-port-number*] [**key** *key-string*] [**priority** *priority*] [**retransmit** *retries*] [**timeout** *timeout*] [**usg-type** {**802.1x** | **all** | **login**}]

no radius-server host *hostname*

Parameters

- *ip-address*—IP address of the RADIUS server.
- *hostname*—Hostname of the RADIUS server.
- **acct-port** *acct-port-number*—(Optional) Specifies the UDP port number of the RADIUS server for accounting requests. If the UDP port number is set to 0, the host is not used for accounting. (Range: 0 to 65535)
- **auth-port** *auth-port-number*—(Optional) Specifies the UDP port number of the RADIUS server for authentication requests. If the UDP port number is set to 0, the host is not used for authentication. (Range: 0 to 65535)
- **key** *key-string*—(Optional) Specifies the authentication and encryption key for all RADIUS communications between the switch and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0 to 128 characters)
- **priority** *priority*—(Optional) Specifies the priority of the RADIUS server, where 0 has the highest priority. (Range: 0 to 65535)
- **retransmit** *retries*—(Optional) Specifies the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. (Range: 1 to 10, default: 3)

- **timeout** *timeout*—(Optional) Specifies the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. If there is no value entered in this field, the switch uses the default timeout value. (Range: 1 to 30, default: 3)
- **usg-type** {**802.1x** | **all** | **login**}—(Optional) Specifies the authentication type of the RADIUS server. The possible values are:
  - **802.1x**—The RADIUS server is used for 802.1x port authentication.
  - **all**—The RADIUS server is used for user login authentication and 802.1x port authentication.
  - **login**—The RADIUS server is used for user login authentication (authenticating users that want to administer the switch).

Default Configuration

The default authentication port number is 1812.

If **timeout** is not specified, the global value (set in the **radius-server default-param** command) is used.

If **retransmit** is not specified, the global value (set in the **radius-server default-param** command) is used.

If **key-string** is not specified, the global value (set in the **radius-server default-param** command) is used.

If a parameter was not set in one of the above commands, the default for that command is used. For example, if a timeout value was not set in the current command, the default timeout set in the **radius-server default-param** command is used.

The default authentication type is **all**.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, this command is used for each host.

Example

The following example specifies a RADIUS server with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period:

```
switchxxxxxx(config)# radius-server host radiusserver1 auth-port 20 timeout
20
```

show radius-server

To show information of the RADIUS servers defined on the switch, use the **show radius-server** Privileged EXEC mode command.

Syntax

show radius-server

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show radius-server
 Prio |    IP Address     | Auth-Port| Retries| Timeout| Usage-Type|    Key
------+-------------------+----------+--------+--------+-----------+---------
    1 |      10.193.22.1 |   1812    |    3    |    3     |     All    |
```

The following table describes the significant fields shown in the example:

Field	Description
Prio	Priority of the RADIUS server, where 0 has the highest priority.
IP Address	IP address or hostname of the RADIUS server.
Auth-Port	UDP port number of the RADIUS server for authentication requests. The value of zero indicates that the host is not used for authentication.
Retries	Number of requests that are sent to the RADIUS server before a failure is considered to have occurred.
Timeout	Number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server.

Field	Description
Usage-Type	Authentication type of the RADIUS server. The possible values are: ▪ 802.1x—The RADIUS server is used for 802.1x port authentication. ▪ all—The RADIUS server is used for user login authentication and 802.1x port authentication. ▪ login—The RADIUS server is used for user login authentication (authenticating users that want to administer the switch).
Key	Authentication and encryption key for all RADIUS communications between the switch and the RADIUS server.

show radius-server default-param

To show the default RADIUS server parameters, use the **show radius-server default-param** Privileged EXEC mode command.

Syntax

show radius-server default-param

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show radius-server default-param
 Retries| Timeout|   Key
--------+--------+---------
     3   |     3   |
```

The following table describes the significant fields shown in the example:

Field	Description
Retries	Default number of requests that are sent to the RADIUS server before a failure is considered to have occurred.
Timeout	Default number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
Key	Default key for authenticating and encrypting the RADIUS communications between the switch and the RADIUS server.

31

RMON Commands

clear rmon statistics

To clear all Remote Monitoring (RMON) statistics or to clear the RMON statistics for a specific interface or for a range of interfaces, use the **clear rmon statistics** Privileged EXEC mode command.

Syntax

clear rmon statistics [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—(Optional) Specifies an interface or a list of interfaces to be sampled.

Command Mode

Privileged EXEC mode

Example

The following example clears the RMON statistics for port 1:

```
switchxxxxxx# clear rmon statistics interfaces gi1
```

rmon alarm

To configure a RMON alarm, use the **rmon alarm** Global Configuration mode command.

To delete a RMON alarm, use the **no** form of this command.

Syntax

rmon alarm *index* **interface** *interface-id* {**variable** *interval* {**absolute** | **delta**}} **rising** *rising-threshold rising-event* **falling** *falling-threshold falling-event* **startup** {**rising** | **rising-falling** | **falling**} [**owner** *NAME*]

no rmon alarm *index*

Parameters

- *index*—Alarm index number. (Range: 1 to 65535)
- **interface** *interface-id*—Specifies the interface to be sampled.
- **variable**—Specifies the MIB object to monitor. The possible values are:
  - **broadcast-pkts**—Broadcast packets.
  - **collisions**—Collision.
  - **crc-align-errors**—CRC alignment error.
  - **drop-events**—Total number of events received in which the packets were dropped.
  - **fragments**—Total number of packet fragment.
  - **jabbers**—Total number of packet jabber.
  - **multicast-pkts**—Multicast packets.
  - **octets**—Octets.
  - **oversize-pkts**—Number of oversized packets.
  - **pkts**—Number of packets.
  - **pkts1024to1518octets**—Number of packets size 1024 to 1518 octets.
  - **pkts512to1023octets**—Number of packets size 512 to 1023 octets.
  - **pkts256to511octets**—Number of packets size 256 to 511 octets.
  - **pkts128to255octets**—Number of packets size 128 to 255 octets.
  - **pkts65to127octets**—Number of packets size 65 to 127 octets.
  - **pkts64octets**—Number of packets size 64 octets.
  - **undersize-pkts**—Number of undersized packets.

- *interval*—The interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1 to 2147483647)
- {**absolute** | **delta**}—Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
  - **absolute**—The selected variable value is compared directly with the thresholds at the end of the sampling interval.
  - **delta**—The selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- *rising-threshold*—The rising threshold value. (Range: 0 to 2147483647)
- *rising-event*—The index of the event triggered when a rising threshold is crossed. (Range: 0 to 65535)
- *falling-threshold*—The falling counter value that triggers the falling threshold alarm. (Range: 0 to 2147483647)
- *falling-event*—The index of the event triggered when a falling threshold is crossed. (Range: 0 to 65535)
- **startup** {**rising** | **rising-falling** | **falling**}—Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - **rising**—A single rising alarm is generated if the first sample (after this entry becomes valid) is greater than or equal to the rising threshold.
  - **rising-falling**—A single rising alarm is generated if the first sample (after this entry becomes valid) is greater than or equal to the rising threshold. If the first sample (after this entry becomes valid) is less than or equal to the falling threshold, a single falling alarm is generated.
  - **falling**—A single falling alarm is generated if the first sample (after this entry becomes valid) is less than or equal to the falling threshold.
- **owner** *NAME*—(Optional) Specifies the name of the user or network management system that receives the RMON alarm.

Default Configuration

The default method type is **absolute**.

The default **startup** direction is **rising-falling**.

If the owner name is not specified, the default is an empty string.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# rmon alarm 1000 interface gi11 collisions 10 delta
rising 100 1 falling 20 2 startup rising owner public
```

rmon event

To configure a RMON event, use the **rmon event** Global Configuration mode command.

To delete a RMON event, use the **no** form of this command.

Syntax

rmon event *index* {**log** | **trap** *COMMUNITY* | **log trap** *COMMUNITY*} [**description** *DESCRIPTION*] [**owner** *NAME*]

no rmon event *index*

Parameters

- *index*—The event index. (Range: 1 to 65535)
- **log**—Specifies that a notification entry is generated in the log table by the switch for this event.
- **trap** *COMMUNITY*—Specifies that an SNMP trap community is sent to one or more management stations by the switch for this event.
- **log trap** *COMMUNITY*—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the switch for this event.
- **description** *DESCRIPTION*—(Optional) Specifies the comment describing this event. (Length: 0 to 127 characters)
- **owner** *NAME*—(Optional) Specifies the name of the person who configured this event.

Default Configuration

If the owner name is not specified, the default is an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an event identified as index 10, for which the switch generates a notification in the log table:

```
switchxxxxxx(config)# rmon event 10 log
```

rmon history

To configure a RMON MIB history on an Ethernet interface, use the **rmon history** Global Configuration command.

To remove a RMON history, use the **no** form of this command.

Syntax

rmon history *index* **interface** *interface-id* [**buckets** *bucket-number*] [**interval** *seconds* | **owner** *NAME*]

no rmon history *index*

Parameters

- *index*—The history index. (Range: 1 to 65535)
- **interface** *interface-id*—Specifies the interface to be sampled.
- **buckets** *bucket-number*—(Optional) Specifies the maximum number of buckets desired for the RMON collection history. (Range: 1 to 50)
- **interval** *seconds*—(Optional) Specifies the interval in seconds during which the data is sampled and compared with the rising and falling thresholds. (Range: 1 to 3600)
- **owner** *NAME*—(Optional) Specifies the name of the person who configured this history.

Default Configuration

The default bucket value is 50.

The default interval value is 180 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# rmon history 1 interface fa11 buckets 50 interval 300
owner john
```

show rmon alarm

To display information for a specific RMON alarm or for all RMON alarms, use the **show rmon alarm** Privileged EXEC mode command.

Syntax

show rmon alarm {**all** | *index*}

Parameters

- **all**—Displays all alarms.
- *index*—Information for a specific RMON alarm. (Range: 1 to 65535)

Command Mode

Privileged EXEC mode

Example

The following example displays information of the RMON alarm 1:

```
switchxxxxxx# 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 example:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	Value of the statistic 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.
Interval	Interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	Method of sampling the variable and calculating the value compared against the thresholds. If the value is absolute, the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is delta, the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Startup Alarm	Alarm that is 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-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-falling, then a single falling alarm is generated.
Rising Threshold	Sampled statistic rising 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.

Falling Threshold	Sampled statistic falling 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.
Rising Event	Event index used when a rising threshold is crossed.
Falling Event	Event index used when a falling threshold is crossed.
Owner	Entity that configured this entry.

show rmon event

To show information for a specific RMON event or for all entries in the RMON event table, use the **show rmon event** Privileged EXEC mode command.

Syntax

show rmon event { **all** | *index*}

Parameters

- **all**—Displays all RMON events.
- *index*—The RMON event index to be displayed. (Range: 1 to 65535)

Command Mode

Privileged EXEC mode

Example

The following example displays all entries in the RMON event table:

```
switchxxxxxx# show rmon event all
Rmon Event Index       : 10
Rmon Event Type        : Log
Rmon Event Community   :
Rmon Event Description :
Rmon Event Last Sent   :  (0) 0:00:00.00
Rmon Event Owner       :
```

The following table describes significant fields shown in the example:

Field	Description
Index	Unique index that identifies this event.
Type	Type of notification that the device generates about this event. The available values are none, log, trap, and log-trap. In the case of log, an entry is made in the log table for each event. In the case of trap, a SNMP trap is sent to one or more management stations.
Community	If a SNMP trap is to be sent, it is sent with the SNMP community string specified by this octet string.
Description	Comment describing this event.
Last Sent	The time that this entry last generated an event. If this entry has not generated any events, this value is zero.
Owner	The entity configured this event.

show rmon event log

To show information for RMON events in the RMON log table, use the **show rmon event log** Privileged EXEC mode command.

Syntax

show rmon event [*index*] **log**

Parameters

- *index*—(Optional) The RMON event index. (Range: 1 to 65535)

Command Mode

Privileged EXEC mode

Example

The following example shows information for the event 1 in the RMON log table:

```
switchxxxxxx# show rmon event 1 log
Maximum table size: 500 (800 after reset)
```

```
Event   Description             Time
-----   --------------          -------------------
1       MIB Var.:               Jan 18 2006 23:48:19
        1.3.6.1.2.1.2.2.1.10.
        53, Delta, Rising,
        Actual Val: 800,
        Thres.Set: 100,
        Interval (sec):1
```

show rmon history

To show information for all RMON histories or for a specific RMON history, use the **show rmon history** Privileged EXEC mode command.

Syntax

show rmon history {**all** | *index* } [**statistic**]

Parameters

- **all**—Displays all histories.
- *index*—The set of samples. (Range: 1 to 65535)
- **statistic**—(Optional) Displays the statistics for a specific RMON history.

Command Mode

Privileged EXEC mode

Example

The following example displays all RMON histories:

```
switchxxxxxx# show rmon history all
Rmon History Index       : 1
Rmon Collection Interface: 11
Rmon History Bucket      : 60
Rmon history Interval    : 300
Rmon History Owner       : john
```

The following table describes the significant fields shown in the example:

Field	Description

Index	The history index.
Collection Interface	The interface to be sampled.
Bucket	The maximum number of buckets desired for the RMON collection history group of statistics.
Interval	The interval in seconds during which the data is sampled and compared with the rising and falling thresholds.
Owner	The name of the person who configured this history.

show rmon statistics interfaces

To show the RMON statistics for all Ethernet interfaces or a specific Ethernet interface, use the **show rmon statistics interfaces** Privileged EXEC mode command.

Syntax

show rmon statistics interfaces *interface-id*

Parameters

- *interface-id*—An interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

The following example displays the RMON statistics for fa1:

```
switchxxxxxx# show rmon statistics interfaces gi1
==== Port gi1 ============================
etherStatsDropEvents            : 0
etherStatsOctets                : 178566
etherStatsPkts                  : 2261
etherStatsBroadcastPkts         : 299
etherStatsMulticastPkts         : 147
etherStatsCRCAlignErrors        : 0
etherStatsUnderSizePkts         : 0
etherStatsOverSizePkts          : 0
```

```
etherStatsFragments             : 0
etherStatsJabbers               : 0
etherStatsCollisions            : 0
etherStatsPkts64Octets          : 1848
etherStatsPkts65to127Octets     : 218
etherStatsPkts128to255Octets    : 170
etherStatsPkts256to511Octets    : 25
etherStatsPkts512to1023Octets   : 0
etherStatsPkts1024to1518Octets  : 0
```

The following table describes the significant fields shown in the example:

Field	Description
Dropped Events	Total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times that this condition was detected.
Octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast Packets	Total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast Packets	Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	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).
Undersize Packets	Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.

Oversize Packets	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	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).
Jabbers	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).
Collisions	Best estimate of the total number of collisions on this Ethernet segment.
64 Octets	Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	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).
128 to 255 Octets	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).
256 to 511 Octets	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).
512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets.

1024 to 1518 Octets	Total number of packets (including bad packets) received that were between 1024 octets and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

32

Security DoS Commands

security-suite dos (Global)

To enable specific Denial of Service (DoS) protections in security suite, use the **security-suite dos** Global Configuration mode command.

To disable specific DoS protections, use the **no** form of this command.

Syntax

security-suite dos {**daeqsa-deny** | **icmp-frag-pkts-deny** | **icmpv4-ping-max-check** | **icmpv6-ping-max-check** | **ipv6-min-frag-size-check** | **land-deny** | **nullscan-deny** | **pod-deny** | **smurf-deny** | **syn-sportl1024-deny** | **synfin-deny** | **synrst-deny** | **tcp-frag-off-min-check** | **tcpblat-deny** | **tcphdr-min-check** | **udpblat-deny** | **xma-deny**}

security-suite dos icmp-ping-max-length *MAX_LEN*

security-suite dos ipv6-min-frag-size-length *MIN_LEN*

security-suite dos smurf-netmask *MASK*

security-suite dos tcphdr-min-length *HDR_MIN_LEN*

no security-suite dos {**daeqsa-deny** | **icmp-frag-pkts-deny** | **icmpv4-ping-max-check** | **icmpv6-ping-max-check** | **ipv6-min-frag-size-check** | **land-deny** | **nullscan-deny** | **pod-deny** | **smurf-deny** | **syn-sportl1024-deny** | **synfin-deny** | **synrst-deny** | **tcp-frag-off-min-check** | **tcpblat-deny** | **tcphdr-min-check** | **udpblat-deny** | **xma-deny**}

Parameters

- **daeqsa-deny**—Drops the packets if the destination MAC address equals to the source MAC address.
- **icmp-frag-pkts-deny**—Drops the fragmented ICMP packets.
- **icmpv4-ping-max-check**—Checks the maximum size of ICMPv4 ping packets and drops the packets larger than the maximum packet size.

- **icmpv6-ping-max-check**—Checks the maximum size of ICMPv6 ping packets and drops the packets larger than the maximum packet size.
- **ipv6-min-frag-size-check**—Checks the minimum size of IPv6 fragments and drops the packets smaller than the minimum size.
- **land-deny**—Drops the packets if the source IP address equals to the destination IP address.
- **nullscan-deny**—Drops the packets with NULL scan.
- **pod-deny**—Avoids ping of death attack.
- **smurf-deny**—Avoids smurf attack.
- **syn-sportl1024-deny**—Drops SYN packets with sport less than 1024.
- **synfin-deny**—Drops the packets with SYN and FIN bits set.
- **synrst-deny**—Drops the packets with SYN and RST bits set.
- **tcp-frag-off-min-check**—Drops the TCP fragment packets with offset equals to one.
- **tcpblat-deny**—Drops TCP fragment packets with offset equals to one.
- **tcphdr-min-check**—Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size.
- **udpblat-deny**—Drops the packets if the source UDP port equals to the destination UDP port.
- **xma-deny**—Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
- **icmp-ping-max-length** *MAX_LEN*—Specifies the maximum size of the ICMPv4/ICMPv6 ping packets. (Range: 0 to 65535 bytes)
- **ipv6-min-frag-size-length** *MIN_LEN*—Specifies the minimum size of IPv6 fragments. (Range: 0 to 65535 bytes)
- **smurf-netmask** *MASK*—Specifies the netmask of smurf attack. (Netmask length range: 0 to 32 bytes)
- **tcphdr-min-length** *HDR_MIN_LEN*—Specifies the minimum TCP header length. (Range: 0 to 31 bytes)

Default Configuration

All types of DoS protection are enabled in security suit by default.

The default parameters are:

- The maximum size of ICMP ping packets is 512 bytes.
- The minimum size of IPv6 fragments is 1240 bytes.
- The Smurf netmask length is 0 bytes.
- The minimum TCP header length is 20 bytes.

Command Mode

Global Configuration mode

Example

The following example enables checking the minimum size of IPv6 fragments and sets the minimum fragment size to 1000 bytes:

```
switchxxxxxx(config)# security-suite dos ipv6-min-frag-size-check
switchxxxxxx(config)# security-suite dos ipv6-min-frag-size-length 1000
```

security-suite dos (Interface)

To enable DoS protections on an interface, use the **security-suite dos** Interface Configuration (Ethernet) mode command.

To disable DoS protections on an interface, use the **no** form of this command.

Syntax

security-suite dos

no security-suite dos

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi6
switchxxxxxx(config-if)# security-suit dos
```

security-suite dos ip gratuitous-arps

To enable gratuitous ARP protection on an interface, use the **security-suite ip gratuitous-arps** Interface Configuration (Ethernet) mode command.

To disable this feature on an interface, use the **no** form of this command.

Syntax

security-suite dos ip gratuitous-arps

no security-suite dos ip gratuitous-arps

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface gi10
switchxxxxxx(config-if)# security-suit dos ip gratuitous-arps
```

show security-suite dos

To show the DoS protection configuration, use the **show security-suite dos** Privileged EXEC Mode command.

Syntax

show security-suite dos

Parameters

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show security-suite dos
  Type                        | State (Length)
------------------------------+---------------------------------
  DMAC equal to SMAC          | enabled
  Land (DIP = SIP)            | enabled
  UDP Blat (DPORT = SPORT)    | enabled
  TCP Blat (DPORT = SPORT)    | enabled
  POD (Ping of Death)         | enabled
  IPv6 Min Fragment Size      | enabled  (1000 Bytes)
  ICMP Fragment Packets       | enabled
  IPv4 Ping Max Packet Size   | enabled  (512 Bytes)
  IPv6 Ping Max Packet Size   | enabled  (512 Bytes)
  Smurf Attack                | enabled  (Netmask Length: 0)
  TCP Min Header Length       | enabled  (20 Bytes)
  TCP Syn (SPORT < 1024)      | enabled
  Null Scan Attack            | enabled
  X-Mas Scan Attack           | enabled
  TCP SYN-FIN Attack          | enabled
  TCP SYN-RST Attack          | enabled
  TCP Fragment (Offset = 1)   | enabled
```

show security-suite dos interfaces

To show the DoS protection and gratuitous ARP protection status per interface, use the **show security-suite dos interfaces** Privileged EXEC Mode command.

Syntax

show security-suite dos interfaces *interface-id*

Parameters

- *interface-id*—An interface ID or a list of interface IDs.

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show security-suite interface gi1-3
  Port    | DoS Protection | Gratuitous-ARP
----------+----------------+----------------
     gi1  |    enabled     |    enabled
     gi2  |    disabled    |    disabled
     gi3  |    disabled    |    disabled
```

33

SNMP Commands

show snmp-server

To show the Simple Network Management Protocol (SNMP) service status, use the **show snmp-server** Privileged EXEC mode command.

Syntax

show snmp-server

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp-server
SNMP is enabled
System Contact : test
System Location : test_location
```

show snmp-server community

To show the SNMP communities defined on the switch, use the **show snmp-server community** Privileged EXEC mode command.

Syntax

show snmp-server community

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp-server community
Community Name      Group Name                    View
Access
-------------------- ------------------------------ ------------------------
------ ------------
test                                              all
ro

Total Entries: 1
```

The following table describes the significant fields shown in the example:

Field	Description
Community Name	SNMP community name.
Group name	SNMP group associated with the SNMP community to determine the access rights.
View	SNMP view that can access the SNMP community. **all** indicates that any IP device can access the SNMP community.

Field	Description
Access	Community access level. The options are: ▪ ro—(Read Only) Management access is restricted to read-only. Changes cannot be made to the community. ▪ rw—(Read Write) Management access is read-write. Changes can be made to the device configuration, but not to the community.

show snmp-server engineid

To show the SNMPv3 engine IDs defined on the switch, use the **show snmp-server engineid** Privileged EXEC command.

Syntax

show snmp-server engineid

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp engineid
Local SNMPV3 Engine id: 00036D001000

     IP address                    Remote SNMP engineID
-------------------------------------------------------------------------------
192.168.1.55                       00036D10000A

Total Entries: 1
```

The following table describes the significant fields shown in the example:

Field	Description
Local SNMPV3 Engine id	Local SNMP engine ID of the switch.
IP address	IP address of the remote host that receives the traps.
Remote SNMP engineID	Remote SNMP engine ID.

show snmp-server group

To show all SNMP groups defined on the switch, use the **show snmp-server group** Privileged EXEC mode command.

Syntax

show snmp-server group

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp-server group
Group Name                      Model  Level        ReadView
  WriteView                       NotifyView
------------------------------ ------ ------------ --------------------------
---- ------------------------------ ------------------------------
testgroup                       v1     noauth       all
  all                             all

Total Entries: 1
```

The following table describes the significant fields shown in the example:

Field	Description
Group Name	SNMP Group name.
Model	SNMP version in use (v1, v2c, or v3).
Level	Packet authentication with encryption (Applicable to SNMPv3 security only). The options are: ▪ noauth—No packet authentication will be performed. ▪ auth—Packet authentication without encryption will be performed. ▪ priv—Packet authentication with encryption will be performed.
ReadView	SNMP view enabling viewing the agent contents. If not specified, all objects except the community-table, SNMPv3 user, and access tables are available.
WriteView	SNMP view enabling data entry and managing the agent contents.
NotifyView	SNMP view enabling receiving the notify object ID for the agent contents. (It's not used for application)

show snmp-server host

To show all SNMP notification recipients defined on the switch, use the **show snmp-server host** Privileged EXEC mode command.

Syntax

show snmp-server host

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp-server host
Server           Community Name   Notification Version    Notification Type
UDP Port    Retries     Timeout
--------------------------------------------------------------------------------
-----------------------------------
10.172.1.1       public          v3                      trap
--          --           --

Total Entries: 1
```

The following table describes the significant fields shown in the example:

Field	Description
Server	IP address or hostname of the SNMP notification recipient.
Community Name	SNMP community of the trap manager.
Notification Version	SNMP version for SNMP traps.
Notification Type	Send traps or informs to the recipients.
UDP Port	UDP port used for notifications on the recipient device.
Retries	Number of times that the switch resends an inform request.
Timeout	Number of seconds that the switch waits before resending informs.

show snmp-server trap

To show whether SNMP traps are enabled or disabled on the switch, use the **show snmp-server trap** Privileged EXEC mode command.

Syntax

show snmp-server trap

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxx# show snmp-server trap
SNMP auth failed trap  : Enable
SNMP linkUpDown trap   : Enable
SNMP warm-start trap   : Enable
SNMP cold-start trap   : Enable
SNMP port security trap: Enable
```

show snmp-server view

To show all SNMP views defined on the switch, use the **show snmp-server view** Privileged EXEC mode command.

Syntax

show snmp-server view

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp-server view
View Name       Subtree OID              OID Mask                 View Type
------------    ----------------------   ----------------------   ---------
all             .1                       all                      included
agon            .1.3.6.1                 all                      included
```

```
Total Entries: 2
```

The following table describes the significant fields shown in the example:

Field	Description
View Name	SNMP view name.
Subtree OID	Subtree Object ID . All descendants of this node are included or excluded in the view.
OID Mask	Object ID mask.
View Type	Shows that the selected MIBs are included or excluded in this view.

show snmp-server user

To show all SNMP users defined on the switch, use the **show snmp-server user** Privileged EXEC mode command.

Syntax

show snmp-server user

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show snmp-server user
Username:                snmpuser
Password:                ********
Access GroupName:        snmpgroup
Authentication Protocol: md5
Encryption Protocol:     none
```

```
Access SecLevel:          auth

Total Entries: 1
```

The following table describes the significant fields shown in the example:

Field	Description
Username	Name of the SNMP user.
Password	MD5 or SHA password or key to authenticate the SNMP user.
Access GroupName	SNMP group to which the SNMP user belongs.
Authentication Protocol	Authentication method. The options are: ▪ none—No user authentication is used. ▪ md5—Use the MD5 protocol to authenticate the SNMP user. ▪ sha—Use the SHA (Secure Hash Algorithm) protocol to authenticate the SNMP user.
Encryption Protocol	Encryption protocol to encrypt the authentication password.
Access SecLevel	Security level attached to the group. The available options are: ▪ noauth—(No Authentication and No Privacy) Neither the Authentication nor the Privacy security levels are assigned to the group. ▪ auth—(Authentication and No Privacy) Authenticates SNMP messages, and ensures that the SNMP message origin is authenticated but does not encrypt them, meaning that they can be intercepted and read. ▪ priv—(Authentication and Privacy) Authenticates SNMP messages, and encrypts SNMP messages if the SNMP message origins are authenticated.

snmp-server

To enable SNMP on the switch, use the **snmp-server** Global Configuration mode command.

To disable SNMP on the switch, use the **no** form of this command.

Syntax

snmp-server

no snmp-server

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server
```

snmp-server community

To define an SNMP community that permits access to SNMP commands (v1 and v2), use the **snmp-server community** Global Configuration mode command.

To delete an SNMP community, use the **no** form of this command.

Syntax

snmp-server community *community-string* [**view** *view-name*] {**ro** | **rw**}

snmp-server community *community-string* **group** *group-name*

no snmp-server community *community-string*

Parameters

- *community-string*—The SNMP community name. The community string is used as an input parameter to **snmp-server user** for SNMPv3. (Range: 0 to 20 characters)
- **view** *view-name*—(Optional) Specifies the SNMP view (configured using the **snmp-server view** command) to define the objects available to the community. It is not relevant for su, which has access to the whole MIB. If unspecified, all objects, except the community-table, SNMPv3 user, and access tables, are available. (Range: 1 to 30 characters)
- **ro**—Read-only access (default).
- **rw**—Read-write access.
- **group** *group-name*—Specifies the SNMP group (configured using the **snmp-server group** command with v1 or v2) to define the objects available to the community. (Range: 1 to 30 characters)

Default Configuration

No SNMP community is defined.

Command Mode

Global Configuration mode

User Guidelines

To associate communities with access rights directly (basic mode), use the **snmp-server community** *community-string* [**view** *view-name*] {**ro** | **rw**} command. The *view-name* value is used to restrict the access rights of a community string. When a view name is specified, the software:

- Generates an internal security name.
- Maps the internal security name for SNMPv1 and SNMPv2 security models to an internal group name.
- Maps the internal group name for SNMPv1 and SNMPv2 security models to the view name (read-view and notify-view always, and for rw for write-view also).

To associate communities with access rights through groups (advanced mode), use the **snmp-server community** *community-string* **group** *group-name* command. The *group-name* value is used to restrict the access rights of a community string. When a group name is specified, the software:

- Generates an internal security name.
- Maps the internal security name for SNMPv1 and SNMPv2 security models to the group name.

Example

The following example defines an SNMP community comm1 and associates it with the group abcd:

```
switchxxxxxx(config)# snmp-server community comm1 group abcd
```

snmp-server contact

To set the system contact, use the **snmp-server contact** Global Configuration mode command.

Syntax

snmp-server contact *contact*

Parameters

- *contact*—The system contact name. (Length: 0 to 256 characters)

Default Configuration

No contact name is defined.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server contact Robert
```

snmp-server engineid

To define a local SNMPv3 engine ID, use the **snmp-server engineid** Global Configuration mode command.

Syntax

snmp-server engineid {**default** | *ENGINEID*}

Parameters

- **default**—Uses the default generated SNMP engine ID.
- *ENGINEID*—Specifies a local SNMP engine ID. The engine ID is a 10 to 64 hexadecimal characters. The hexadecimal number must be divided by 2.

Default Configuration

The default SNMP engine ID is based on the MAC address of the switch.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server engineid 00036D001122
```

snmp-server engineid remote

To define a remote host for the SNMP engine, use the **snmp-server engineid remote** Global Configuration mode command.

Syntax

snmp-server engineid remote *host-ip ENGINEID*

Parameters

- *host-ip*—The IP address or hostname of the remote host (the targeted recipient). The default is all IP addresses.
- *ENGINEID*—The remote SNMP engine ID. The engine ID is a 10 to 64 hexadecimal characters. The hexadecimal number must be divided by 2.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server engineid remote 172.10.77.1 00036D0012
```

snmp-server group

To define an SNMP group, use the **snmp-server group** Global Configuration mode command. Groups are used to map SNMP users to SNMP views (using the **snmp-server user** command).

To delete an SNMP group, use the **no** form of this command.

Syntax

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

no snmp-server group *groupname* {**v1** | **v2c** | **v3**} {**noauth** | **auth** | **priv**}

Parameters

- *groupname*—The SNMP group name. (Length: 1 to 30 characters)
- {**v1** | **v2c** | **v3**}—Specifies the SNMP version.
- **noauth**—Specifies that no packet authentication will be performed. Applicable only to the SNMP version 3 security model.
- **auth**—Specifies that packet authentication without encryption will be performed. Applicable only to the SNMP version 3 security model.
- **priv**—Specifies that packet authentication with encryption will be performed. Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.

- **read-view** *readview*—Sets the view name that enables viewing only. (Length: 1 to 30 characters)
- **write-view** *writeview*—Sets the view name that enables configuring the agent. (Length: 1 to 30 characters; setting "" means no write view)
- **notify-view** *notifyview*—(Optional) Sets the view name that sends only traps with contents that is included in SNMP view selected for notification. Otherwise, there is no restriction on the contents of the traps. This can only be available for SNMPv3. (Length: 1 to 30 characters)

Default Configuration

No group entry exists.

If the *notifyview* value is not specified, the notify view is not defined.

If the *readview* value is not specified, all objects except for the community table, SNMPv3 user, and access tables are available for retrieval.

If the *writeview* value is not specified, the write view is not defined.

Command Mode

Global Configuration mode

User Guidelines

The group defined in this command is used in the **snmp-server user** command to map SNMP users to the SNMP group. These users are then automatically mapped to SNMP views defined in this command.

The security level for SNMP v1 or v2 is always **noauth**.

Example

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read-view view1
write-view view2
```

snmp-server host

To configure the hosts to receive SNMP notifications (traps or informs), use the **snmp-server host** Global Configuration mode command.

To delete an SNMP notification recipient, use the **no** form of this command.

Syntax

snmp-server host {*ipv4address* | *hostname* | *ipv6address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3**} [**noauth** | **auth** | **priv**]] *community-string* [**udp-port** *port-number*] [**timeout** *timeout-value*] [**retries** *retry-time*]

no snmp-server host {*ipv4address* | *hostname* | *ipv6address*}

Parameters

- *ipv4address*—IPv4 address of the host (the targeted recipient). The default is all IP addresses.
- *hostname*—Hostname of the host (the targeted recipient).
- *ipv6address*—IPv6 address of the host (the targeted recipient). The default is all IP addresses.
- **traps**—(Optional) Sends SNMP traps to the host. This is the default setting.
- **informs**—(Optional) Sends SNMP informs to the host.
- **version** {**1** | **2c** | **3**}—(Optional) Specifies the SNMP version.
  - **1**—SNMPv1 traps are used.
  - **2c**—SNMPv2 traps or informs are used.
  - **3**—SNMP version 3 is used.
- **noauth**—(Optional) Specifies that no packet authentication will be performed. Applicable only to the SNMP version 3 security model.
- **auth**—(Optional) Specifies that packet authentication without encryption will be performed. Applicable only to the SNMP version 3 security model.
- **priv**—(Optional) Specifies that packet authentication with encryption will be performed. Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.
- *community-string*—The SNMP community sent with the notification operation. For SNMP v1 and v2, any community string can be entered here. (Range: 1 to 20 characters)
- **udp-port** *port-number*—(Optional) Specifies the UDP port number.
- **timeout** *timeout-value*—(Optional) Specifies the SNMP inform timeout.
- **retries** *retry-time*—(Optional) Specifies the number of SNMP inform retries.

Default Configuration

The default SNMP version is SNMPv1.

Command Mode

Global Configuration mode

User Guidelines

Use the **snmp-server user**, **snmp-server group**, and **snmp-server view** commands to create a SNMP user, a SNMP group, or a SNMP view.

Example

```
switchxxxxxx(config)# snmp-server host 1.1.1.121 abc
```

snmp-server location

To set the system location, use the **snmp-server location** Global Configuration mode command.

Syntax

snmp-server location *location*

Parameters

- *location*—The system location. (Length: 0 to 256 characters)

Default Configuration

No location name is defined.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server location NewYork
```

snmp-server trap

To send SNMP traps when the authentication fails, use the **snmp-server trap** Global Configuration mode command.

To disable SNMP traps, use the **no** form of this command.

Syntax

snmp-server trap [**auth** | **cold-start** | **linkUpDown** | **port-security** | **warm-start**]

no snmp-server trap [**auth** | **cold-start** | **linkUpDown** | **port-security** | **warm-start**]

Parameters

- **auth**—(Optional) Enables the SNMP authentication failure trap.
- **cold-start**—(Optional) Enables the SNMP bootup cold startup trap.
- **linkUpDown**—(Optional) Enables the SNMP link up and down trap.
- **port-security**—(Optional) Enables the port security trap.
- **warm-start**—(Optional) Enables the SNMP bootup warm startup trap.

Default Configuration

SNMP auth, cold-start, warm-start, port-security, and linkUpDown traps are enabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server trap auth
```

snmp-server user

To define an SNMP user, use the **snmp-server user** Global Configuration mode command.

To delete an SNMP user, use the **no** form of the command.

Syntax

snmp-server user *username groupname* [**auth** {**md5** | **sha**} *AUTHPASSWD*]

snmp-server user *username groupname* **auth** {**md5** | **sha**} *AUTHPASSWD* **priv** *PRIVPASSWD*

no snmp-server user *username*

Parameters

- *username*—Specifies the name of the user on the host that connects to the SNMP agent. (Range: 1 to 30 characters). For SNMP v1 or v2c, this username must match the community string entered in the **snmp-server host** command.
- *groupname*—Specifies the SNMP group to which the SNMP user belongs. The SNMP group should be configured using the **snmp-server group** command with v1 or v2c parameters. (Range: 1 to 30 characters)
- **auth** {**md5** | **sha**}—(Optional) Specifies the protocol to authenticate the SNMP user. The options are:
  - **md5**—Uses the HMAC-MD5-96 authentication protocol.
  - **Sha**—Uses the HMAC-SHA-96 authentication protocol.
- *AUTHPASSWD*—(Optional) The authentication password. (Length: 8 to 32 characters)
- **priv** *PRIVPASSWD*—Specifies the private password for the privacy key. (Length: 8 to 64 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server user tom acbd
```

snmp-server view

To define an SNMP view, use the **snmp-server view** Global Configuration mode command.

To delete an SNMP view, use the **no** form of this command.

Syntax

snmp-server view *view-name* **subtree** *oid-tree* **oid-mask** {**all** | *MASK*} **viewtype** {**included** | **excluded**}

no snmp-server view *view-name* **subtree** [*oid-tree* | **all**]

Parameters

- *view-name*—The SNMP view name. (Length: 1 to 30 characters)
- **subtree** *oid-tree*—Specifies the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP 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 and, optionally, a sequence of numbers. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4. This parameter depends on the MIB being specified.
- **oid-mask** {**all** | *MASK*}—Specifies the family mask. It is used to define a family of view subtrees. For example, OID mask is 11111010.10000000. The length of the OID mask must be less than the length of subtree OID.
- **viewtype included**—Includes the selected MIBs in the view.
- **viewtype excluded**—Excludes the selected MIBs in the view.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same SNMP view.

The command's logical key is the pair (*view-name*, *oid-tree*). Two commands cannot have the same *view-name* and *oid-tree*.

The number of SNMP views is limited to 16.

Example

```
switchxxxxxx(config)# ssnmp-server view agon subtree 1.3.6.1 oid-mask all
viewtype included
switchxxxxxx(config)# snmp-server view userview subtree 1.3.6.1.2 oid-mask
1111110 viewtype excluded
```

34

STP Commands

clear spanning-tree detected-protocols

To restart the Spanning Tree Protocol (STP) migration process (force renegotiation with neighboring switches) on all interfaces or on a specific interface, use the **clear spanning-tree detected-protocols** Interface Configuration mode command.

Syntax

clear spanning-tree detected-protocols [**interfaces** *interface-id*]

Parameters

- **interfaces** *interface-id*—An interface ID or a list of interface IDs.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

This feature can only be used when the switch is in RSTP or MSTP mode.

Example

```
switchxxxxxx# clear spanning-tree detected-protocols
```

instance (MST)

To map VLANs to a Multiple Spanning Tree Protocol (MSTP) instance, use the **instance** MST Configuration mode command.

To revert to its default settings, use the **no** form of this command.

Syntax

instance *instance-id* **vlan** *vlan-range*

no instance *instance-id* **vlan** *vlan-range*

Parameters

- *instance-id*—The MSTP instance ID. (Range: 0 to 15)
- **vlan** *vlan-range*—Adds a range of VLANs to the MSTP instance. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1 to 4094)

Default Configuration

All VLANs are mapped to the Common and Internal Spanning Tree (CIST) instance (instance 0).

Command Mode

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MSTP instance are mapped to the CIST instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MSTP region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps a range of VLANs to the MSTP instance 1:

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
```

name (MST)

To define the name for an MSTP instance, use the **name** MST Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

name *string*

no name

Parameters

- *string*—The MSTP instance name. (Length: 1 to 32 characters)

Default Configuration

The default MSTP name is the bridge MAC address.

Command Mode

MST Configuration mode

Example

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

revision (MST)

To define the revision number for current MSTP configuration, use the **revision** MST Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

revision *value*

no revision

Parameters

- *value*—Specifies an unsigned 16-bit number that identifies the revision of the current MSTP configuration. (Range: 0 to 65535)

Default Configuration

The default revision number is 0.

Command Mode

MST Configuration mode

Example

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# revision 1
```

show spanning-tree

To show the STP configuration, use the **show spanning-tree** Privileged EXEC mode command.

Syntax

show spanning-tree

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode STP
Default port cost method: short
Loopback guard:  Disabled
```

```
Root ID Priority 32768
Address 64:d8:14:5d:6d:36
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 2 last change occurred 04:57:14 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15

Interfaces
Name State Prio.Nbr Cost Sts Role PortFast Type
--------- -------- -------- -------- ------ ---- -------- -----------------
fa22 enabled 128.22 19 Frw Desg No P2P (STP)
```

show spanning-tree interfaces

To show the STP statistics for specific interfaces, use the **show spanning-tree interfaces** Privileged EXEC mode command.

Syntax

show spanning-tree interfaces *interface-id* [**statistic**]

Parameters

- *interface-id*—An interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.
- **statistic**—(Optional) Displays the STP statistics for the specified interfaces.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example shows the STP information of gi1:

```
switchxxxxxx# show spanning-tree interfaces gi1

Port gi1 enabled
State: disabled                                  Role: disabled
Port id: 128.1                                   Port cost: 200000
Type: Shared Boundary                            Port Fast: No
Designated bridge Priority : 0                   Address: 00:00:00:00:00:00
Designated port id:   0.0                        Designated path cost: 0
BPDU Filter: Disabled                            BPDU guard: Disabled
```

```
BPDU: sent 0, received 0
```

Example 2—The following example shows the STP statistics of gi1:

```
switchxxxxxx# show spanning-tree interfaces gi1 statistic

 STP Port Statistic
================================================

Port                             : fa1
Configuration BDPUs Received     : 0
TCN BDPUs Received               : 8
MSTP BDPUs Received              : 15
Configuration BDPUs Transmitted  : 86696
TCN BDPUs Transmitted            : 0
MSTP BDPUs Transmitted           : 0
```

show spanning-tree mst

To show the MSTP instance information, use the **show spanning-tree mst** Privileged EXEC mode command.

Syntax

show spanning-tree mst *instance-id*

Parameters

- *instance-id*—The MSTP instance ID. (Range: 0 to 15)

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show spanning-tree mst 1

 MST Instance Information
============================================================
            Instance Type : MSTI (1)
          Instance Status : Disabled
        Bridge Identifier : 32768/ 0/00:03:6D:00:10:00
------------------------------------------------------------
     Regional Root Bridge : 32768/ 0/00:03:6D:00:10:00
```

```
  Internal Root Path Cost : 0
          Remaining Hops : 20
        Topology changes : 4
     Last Topology Change : 0
---------------------------------------------------------
 VLANs mapped: 1-4094
=========================================================

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
gi1              Desg FWD 200000    128.1    P2P (STP)
```

show spanning-tree mst configuration

To show the MSTP instance configuration, use the **show spanning-tree mst configuration** Privileged EXEC mode command.

Syntax

show spanning-tree mst configuration

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show spanning-tree mst configuration
Name      [00:03:6D:00:10:A0]
Revision  0     Instances configured 2

Instance  Vlans mapped
--------  -------------------------------------------------------------------
0           1,5-4094
1           2-4
-------------------------------------------------------------------------------
```

show spanning-tree mst interfaces

To show the MSTP instance information for specific interfaces, use the **show spanning-tree mst interfaces** Privileged EXEC mode command.

Syntax

show spanning-tree mst *instance-id* **interfaces** *interface-id*

Parameters

- *instance-id*—The MSTP instance ID. (Range: 0 to 15)
- *interface-id*—An interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show spanning-tree mst 1 interfaces gi1

 MST Port Information
================================================================
 Instance Type : MSTI (1)
----------------------------------------------------------------

      Port Identifier : 128/1
   Internal Path-Cost : 0        /200000
----------------------------------------------------------------
    Regional Root Bridge : 0/00:00:00:00:00:00
      Internal Root Cost : 0
       Designated Bridge : 0/00:00:00:00:00:00
 Internal Port Path Cost : 200000
               Port Role : Disabled
              Port State : Disabled
----------------------------------------------------------------
```

spanning-tree

To enable STP on the switch, use the **spanning-tree** Global Configuration mode command.

To disable STP on the switch, use the **no** form of this command.

Syntax

spanning-tree

no spanning-tree

Parameters

N/A

Default Configuration

STP is enabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# spanning-tree
```

spanning-tree bpdu (Global)

To define Bridge Protocol Data Unit (BPDU) handling when STP is disabled globally, use the **spanning-tree bpdu** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree bpdu {**filtering** | **flooding**}

no spanning-tree bpdu

Parameters

- **filtering**—Filters BPDU packets when STP is disabled globally.

- **flooding**—Floods BPDU packets unconditionally.

Default Configuration

The default setting is **flooding**.

Command Mode

Global Configuration mode

User Guidelines

The filtering and flooding modes are relevant when STP is disabled globally or on a single interface.

Example

```
switchxxxxxx(config)# spanning-tree bpdu flooding
```

spanning-tree bpdu-filter (Interface)

To define BPDU filtering when STP is enabled globally or on a single interface, use the **spanning-tree bpdu-filter** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree bpdu-filter {**disable** | **enable**}

no spanning-tree bpdu-filter

Parameters

- **disable**—Specifies that the interface sends and receives BPDU packets normally.
- **enable**—Specifies that the interface does not send BPDU packets and filters the received BPDU packets.

Default Configuration

BPDU filter is disabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# spanning-tree bpdu-filter enable
```

spanning-tree bpdu-guard (Interface)

To shut down an interface when it receives a BPDU, use the **spanning-tree bpdu-guard** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree bpdu-guard {**disable** | **enable**}

no spanning-tree bpdu-guard

Parameters

- **disable**—Disables BPDU guard.
- **enable**—Enables BPDU guard.

Default Configuration

BPDU guard is disabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

The command can be enabled when STP is enabled globally and on the interface.

Example

The following example shuts down fa5 when it receives an BPDU:

```
switchxxxxxx(config)# interface gi5
```

```
switchxxxxxx(config-if)# spanning-tree bpdu-guard enable
```

spanning-tree cost (Interface)

To configure the STP path cost for an interface, use the **spanning-tree cost** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

Parameters

- *cost*—The port path cost. (Range: 0 to 200000000, 0 indicates Auto)

Default Configuration

The default path cost is determined by the port speed and the path cost method (long or short):

Interface	Long	Short
port channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example configures the STP path cost on fa15 to 35000:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# spanning-tree cost 35000
```

spanning-tree forward-time

To configure the STP bridge forward delay time, which is the amount of time that a port remains in the listening and learning states before entering the forwarding state, use the **spanning-tree forward-time** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Parameters

- *seconds*—The STP forward delay time. (Range: 4 to 30 seconds)

Default Configuration

15 seconds

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be maintained:

2*(Forward-Time - 1) >= Max-Age

Example

```
switchxxxxxx(config)# spanning-tree forward-time 25
```

spanning-tree hello-time

To configure how often the switch broadcasts the hello messages to other devices, use the **spanning-tree hello-time** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Parameters

- *seconds*—The STP hello time in seconds. (Range: 1 to 10)

Default Configuration

2 seconds

Command Mode

Global Configuration mode

User Guidelines

When configuring the hello time, the following relationship should be maintained:

Max-Age >= 2*(Hello-Time + 1)

Example

```
switchxxxxxx(config)# spanning-tree hello-time 5
```

spanning-tree link-type (Interface)

To specify the RSTP link type for an interface, use the **spanning-tree link-type** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

Parameters

- **point-to-point**—Specifies that the port link type is point-to-point.
- **shared**—Specifies that the port link type is shared.

Default Configuration

The default is shared.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# spanning-tree link-type point-to-point
```

spanning-tree loopback-guard

Use the **spanning-tree loopback-guard** Global Configuration command to shutdown an interface if it receives a loopback BPDU.

Use the **no** form of this command to return the default setting.

Syntax

spanning-tree loopback-guard

no spanning-tree loopback-guard

Parameters

N/A

Default Configuration

Spanning-tree loopback guard is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables shutting down all interfaces on which a loopback BPDU is received.

Example

The following example enables shutting down all interfaces on which a loopback BPDU is received:

```
switchxxxxxx(config)# spanning-tree loopback-guard
```

spanning-tree mst port-priority

To configure the priority of a port, use the **spanning-tree mst port-priority** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Parameters

- *instance-id*—The spanning tree instance ID. (Range: 0 to 15)
- *priority*—The port priority. (Range: 0 to 240)

Default Configuration

The default port priority is 128.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the port priority of gi1 to 144:

```
switchxxxxxx(config)# interface gi1
```

```
switchxxxxxx(config-if)# spanning-tree mst 1 port-priority 144
```

spanning-tree max-hops

To configure the number of hops in an MSTP region before BDPU is discarded and the port information is aged out, use the **spanning-tree max-hops** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameters

- *hop-count*—The number of hops in an MSTP region before BDPU is discarded. (Range: 1 to 40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# spanning-tree mst max-hops 10
```

spanning-tree max-age

To set the interval in seconds that the switch can wait without receiving a configuration message before attempting to redefine its own configuration, use the **spanning-tree max-age** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

Parameters

- *seconds*—The interval in seconds that the switch can wait without receiving a configuration message, before attempting to redefine its own configuration. (Range: 6 to 40)

Default Configuration

The default value is 20 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the maximum age, the following relationships should be maintained:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example

```
switchxxxxxx(config)# spanning-tree max-age 10
```

spanning-tree mode

To set the STP mode, use the **spanning-tree mode** Global Configuration mode command.

Syntax

spanning-tree mode {**mstp** | **rstp** | **stp**}

Parameters

- **mstp**—Enables the Multiple STP (MSTP) mode.

- **rstp**—Enables the Rapid STP (RSTP) mode.
- **stp**—Enables the classic STP mode.

Default Configuration

The default mode is classic STP.

Command Mode

Global Configuration mode

User Guidelines

In the RSTP mode, the switch uses STP when the neighbor device uses STP.

In the MSTP mode, the switch uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

```
switchxxxxxx(config)# spanning-tree mode mstp
```

spanning-tree mst configuration

To enter the MST Configuration mode and enable configuring an MSTP region, use the **spanning-tree mst configuration** Global Configuration mode command.

Syntax

spanning-tree mst configuration

Command Mode

Global Configuration mode

User Guidelines

For two or more switches to be in the same MSTP region, they must contain the same VLAN mapping, the same configuration revision number, and the same name.

Example

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
switchxxxxxx(config-mst)# name region1
switchxxxxxx(config-mst)# revision 1
```

spanning-tree mst cost

To configure the path cost for MSTP calculations, use the **spanning-tree mst cost** Interface Configuration mode command. If a loop occurs, the STP considers the path cost when selecting an interface to put in the Forwarding state.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Parameters

- *instance-id*—The MSTP instance ID. (Range: 0 to 15)
- *cost*—The port path cost. (Range: 1 to 200000000, 0 means Auto)

Default Configuration

The default path cost is determined by the port speed and the path cost method (long or short):

Interface	Long	Short
port channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

```
switchxxxxxx(config)# interface gi9
switchxxxxxx(config-if)# spanning-tree mst 1 cost 4
```

spanning-tree mst priority

To configure the device priority for the specified STP instance, use the **spanning-tree mst priority** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Parameters

- *instance-id*—The STP instance ID. (Range: 0 to 15)
- *priority*—The priority for the specified STP instance. This setting ensures the probability that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0 to 61440)

Default Configuration

The default priority is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the STP.

Example

```
switchxxxxxx(config)# spanning-tree mst 1 priority 4096
```

spanning-tree pathcost method

To set the default path cost method, use the **spanning-tree pathcost method** Global Configuration mode command.

Syntax

spanning-tree pathcost method {**long** | **short**}

Parameters

- **long**—The default port path costs are within the range 1 through 200,000,000.
- **short**—The default port path costs are within the range 1 through 65,535.

Default Configuration

Long path cost method

Command Mode

Global Configuration mode

User Guidelines

This command applies to all STP instances on the switch.

- If the short method is selected, the switch calculates cost in the range 1 through 65,535.
- If the long method is selected, the switch calculates cost in the range 1 through 200,000,000.

Example

The following example sets the default path cost method to Long:

```
switchxxxxxx(config)# spanning-tree pathcost method long
```

spanning-tree portfast

To enable the PortFast mode on an interface, use the **spanning-tree portfast** Interface Configuration mode command.

To disable the PortFast mode on an interface, use the **no** form of this command.

Syntax

spanning-tree portfast

no spanning-tree portfast

Parameters

N/A

Default Configuration

The PortFast mode is disabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

In the PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward delay time.

Example

The following example enables the PortFast mode on gi15:

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# spanning-tree portfast
```

spanning-tree port-priority

To configure the STP priority for an interface, use the **spanning-tree port-priority** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

Parameters

- *priority*—The port priority. (Range: 0 to 240)

Default Configuration

The default port priority is 128.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

The priority value must be a multiple of 16.

Example

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# spanning-tree port-priority 96
```

spanning-tree priority

To configure the device STP priority used to determine which bridge is selected as the root bridge, use the **spanning-tree priority** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

Parameters

- *priority*—The bridge priority. (Range: 0 to 61440)

Default Configuration

The default priority is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096. The switch with the lowest priority is the root of the STP. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.

Example

```
switchxxxxxx(config)# spanning-tree priority 12288
```

spanning-tree tx-hold-count

To set the Tx-Hold-Count used to limit the maximum transmission packet number per second, use the **spanning-tree tx-hold-count** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

spanning-tree tx-hold-count *value*

no spanning-tree tx-hold-count

Parameters

- *value*—The Tx-Hold-Count number. (Range: 1 to 10)

Default Configuration

The default value is 6.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config) # spanning-tree tx-hold-count 5
```

SYN Protection Commands

security-suite syn protection mode

To protect TCP SYN attacks and set its protection mode, use the **security-suite syn protection mode** Global Configuration mode command.

Syntax

security-suite syn protection mode {**block** | **disabled** | **report**}

Parameters

- **block—**Blocks the TCP SYN traffic from attacking ports destined to the local system, and generates a rate-limited syslog message.
- **disabled—** Disables the SYN protection feature.
- **report—**Reports for the SYN protection feature about TCP SYN traffic per port (including rate-limited syslog message when an attack is identified).

Default Configuration

The default mode is **block**.

Command Mode

Global Configuration mode

Example

The following example enables SYN protection in block mode on the switch:

```
switchxxxxxx(config)# security-suite syn protection mode block
```

security-suite syn protection recovery

To set the time period for SYN protection to block an attacked interface, use the **security-suite syn protection recovery** Global Configuration mode command.

Syntax

security-suite syn protection recovery *seconds*

Parameters

- *seconds*—The timeout in seconds by which an interface from which SYN packets are blocked gets unblocked. Note that if a SYN attack is still active on this interface, it may become blocked again. (Range: 10 to 600 seconds)

Default Configuration

The default timeout is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

If the timeout is modified, the new value is only used on interfaces that are not currently under attack.

Example

The following example sets the SYN protection auto-recovery timeout to 100 seconds:

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

security-suite syn protection threshold

To set the SYN protection threshold, use the **security-suite syn protection threshold** Global Configuration mode command.

Syntax

security-suite syn protection threshold *pps*

Parameters

- *pps*—The number of packets per second from a specific port that triggers identification of TCP SYN attack. (Range: 20 to 60 packets per second)

Default Configuration

The default SYN protection threshold is 60 packets per second.

Command Mode

Global Configuration mode

Example

The following example sets the SYN protection threshold to 40 packets per second:

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```

show security-suite syn protection

To show the SYN protection settings and the operational status per interface, use the **show security-suite syn protection** Privileged EXEC Mode command.

Syntax

show security-suite syn protection

Parameters

N/A

Command Mode

Privileged EXEC Mode

Example

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 80
Recovery : 60
```

```
 Interface   Operational                    Last Attack
 Name        Status
----------- ------------ ------------------------------------------
    gi13       Normal      00:57:11 01-Jan-2000 blocked and reported
```

The following table describes the significant fields shown in the example:

Field	Description
Protection Mode	Action when the SYN flood attack is detected. ▪ Block—The TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited syslog message is generated. ▪ Disabled—The SYN protection feature is disabled. ▪ Report—The TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited syslog message is generated. The SYN protection feature reports about TCP SYN traffic per port (including rate-limited syslog message when an attack is identified).
Threshold	Number of packets per second from a specific port that triggers identification of TCP SYN attack.
Recovery	Auto-recovery timeout by which a port from which SYN packets are blocked gets unblocked.
Interface Name	Interface identifier.
Operational Status	Shows that SYN protection is enabled or disabled on the interface.
Last Attack	Time of the last SYN flood attack detected on the interface.

36

Syslog Commands

clear logging

To clear the log messages from the internal logging buffer, use the **clear logging** Privileged EXEC mode command.

Syntax

clear logging {**buffered** | **file**}

Parameters

- **buffered**—Clears the log messages stored in RAM.
- **file**—Clears the log messages stored in flash.

Command Mode

Privileged EXEC mode

Example

The following example clears the log messages stored in RAM:

```
switchxxxxxx# clear logging buffered
```

logging host

To define a remote SYSLOG server where log messages are sent (using the SYSLOG protocol), use the **logging host** Global Configuration mode command.

To delete a SYSLOG server, use the **no** form of this command.

Syntax

logging host {*ipv4-address* | *ipv6-address* | *hostname*} [**facility** *facility*] [**port** *port*] [**severity** *severity_level*]

no logging host {*ip-address* | *ipv6-address* | *hostname*}

Parameters

- *ipv4-address*—IPv4 address of the SYSLOG server.
- *ipv6-address*—IPv6 address of the SYSLOG server.
- *hostname*—Hostname of the SYSLOG server. Only translation to IPv4 addresses is supported.
- **facility** *facility*—(Optional) Specifies the log facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, and local7. The default is local7.
- **port** *port*—(Optional) Specifies the port number for SYSLOG messages. The default port number is 514. (Range: 0 to 65535)
- **severity** *level*—(Optional) Specifies the severity of log messages sent to the SYSLOG server. The optional severity levels are:

```
<0-7>          Minimum severity <0-7> (EMEGR-DEBUG)
emergencies    System is unusable
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
errors         Error conditions                  (severity=3)
warnings       Warning conditions                (severity=4)
notifications  Normal but significant conditions (severity=5)
informational  Informational messages            (severity=6)
debugging      Debugging messages                (severity=7)
```

Default Configuration

No messages are logged to a SYSLOG server.

The default severity level is Informational.

Command Mode

Global Configuration mode

User Guidelines

You can specify multiple SYSLOG servers.

Example

```
switchxxxxxx(config)# logging host 1.1.1.121
switchxxxxxx(config)# logging host 3000::100
switchxxxxxx(config)# logging host SYSLOG1
```

logging on

To enable logging on the switch, use the **logging on** Global Configuration mode command.

To disable logging on the switch, use the **no** form of this command.

Syntax

logging on

no logging on

Parameters

N/A

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command sends debug or error messages asynchronously to the designated locations.

The logging process controls the logging message distribution at various destinations, such as the logging buffer, logging file, or SYSLOG server. Logging on and off at these destinations can be individually configured using the **logging console**, **logging buffered**, **logging file**, and **logging host** Global Configuration mode commands.

However, if logging is disabled, no messages are sent to these destinations. Only the console receives the error messages.

Example

The following example enables logging on the switch:

```
switchxxxxxx(config)# logging on
```

logging severity

To set the severity level for error messages that are logged to RAM or flash, use the **logging severity** Global Configuration mode command.

Syntax

logging {**buffered** | **console** | **file**} **severity** [*severity_level*]

Parameters

- **buffered**—Stores the messages in the RAM.
- **console**—Stores the messages on the console.
- **file**—Stores the messages in flash memory.
- *severity_level*—(Optional) The severity level of messages logged in the buffer. The optional severity levels are:

```
<0-7>          Minimum severity <0-7> (EMEGR-DEBUG)
emergencies    System is unusable
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
errors         Error conditions                  (severity=3)
warnings       Warning conditions                (severity=4)
notifications  Normal but significant conditions (severity=5)
informational  Informational messages            (severity=6)
debugging      Debugging messages                (severity=7)
```

Default Configuration

The default severity level is informational.

Command Mode

Global Configuration mode

User Guidelines

All SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example sets the severity level for logging messages to RAM and flash as debugging:

```
switchxxxxxx(config)# logging buffered severity 7
```

show logging

To display the logging status and SYSLOG messages stored in the internal buffer, use the **show logging** Privileged EXEC mode command.

Syntax

show logging [**buffered** | **file**]

Parameters

- **buffered**—(Optional) Displays the log messages stored in the RAM.
- **file**—(Optional) Displays the log messages stored in flash memory.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

Example 1—The following example displays the logging status:

```
switchxxxxxx# show logging
```

```
Logging service is enabled

Console Logging: level notice
Buffer Logging : level info
File Logging   : disabled


Buffer Logging
--------------
*Jan 01 2000 08:04:42: AAA-5: New console connection for user cisco, source
async  ACCEPTED
*Jan 01 2000 08:01:21: STP-6: GigabitEthernet13 STP port state is set to
Forwarding
*Jan 01 2000 08:01:07: STP-6: GigabitEthernet13 STP port state is set to
Learning
*Jan 01 2000 00:00:50: System-5: System Startup!
*Jan 01 2000 00:00:50: System-5: Logging is enabled
```

The following table describes the significant fields shown in the example:

Field	Description
TARGET	Where the log messages are stored.
STATUS	Shows whether RAM memory logging or flash memory logging is enabled or disabled.
Server (PORT)	Server address and port number for SYSLOG messages.
FACILITY	What kind of events are logged.
LOG LEVEL	Severity level of messages to be logged.

Example 2—The following example shows information of the SYSLOG messages stored in the RAM:

```
switchxxxxxx# show logging buffered

                        Log messages in buffered

 NO.|   Timestamp    |    Category    | Severity |  Message
--------------------+----------------+----------+--------------------------
--------------
   1| Jan 01 14:31:24|             AAA|      info| User 'cisco' enter
privileged mode from console with level '15' success
   2| Jan 01 14:31:22|             AAA|      info| User 'cisco' is authorized
with privilege level 15
```

```
   3| Jan 01 14:31:22|              AAA|      info| User 'cisco' login from
console success
   4| Jan 01 14:20:40|              AAA|      info| User 'cisco' enter
privileged mode from telnet with level '15' success
   5| Jan 01 14:20:38|              AAA|      info| User 'cisco' is authorized
with privilege level 15
   6| Jan 01 14:20:38|              AAA|      info| User 'cisco' login from
telnet success
   7| Jan 01 00:30:43|              AAA|      info| User 'cisco' enter
privileged mode from telnet with level '15' success
   8| Jan 01 00:30:36|              AAA|      info| User 'cisco' is authorized
with privilege level 15
   9| Jan 01 00:30:36|              AAA|      info| User 'cisco' login from
telnet success
  10| Jan 01 00:00:55|              STP|      info| Port 1 STP port state is
set to Forwarding
  11| Jan 01 00:00:40|              STP|      info| Port 1 STP port state is
set to Learning
  12| Jan 01 00:00:22|           System|      info| Sysinfo variable
'resetdefault' is set to value '0'
```

The following table describes the significant fields shown in the example:

Field	Description
NO.	Log entry number.
Timestamp	Time when the log message was generated.
Category	Log facility to which the event belongs.
Severity	Severity level of the event.
Message	Description of the log message, indicating what event is logged.

37

System Management Commands

hostname

To modify the hostname of the switch, use the **hostname** Global Configuration mode command.

Syntax

hostname *name*

Parameters

- *name*—The hostname of the switch.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# hostname enterprise
enterprise(config)#
```

ping

To send ICMP echo request packets to another node on the network, use the **ping** Privileged EXEC mode command.

Syntax

ping ip {*ipv4-address* | *hostname*} [**count** *packet_count*]

ping ipv6 {*ipv6-address* | *hostname*} [**count** *packet_count*]

Parameters

- *ipv4-address*—IPv4 address to ping.
- *ipv6-address*—Unicast or multicast IPv6 address to ping.
- *hostname*—Hostname to ping.
- **count** *packet_count*—(Optional) Specifies the number of packets to send. The default is 4 packets. (Range: 1 to 65535)

Default Usage

N/A

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example pings an IP address:

```
switchxxxxxx# ping ip 10.1.1.1
PING 10.1.1.1 (10.1.1.1): 56 data bytes

--- 10.1.1.1 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

Example 2—The following example pings a site:

```
switchxxxxxx# ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] 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
```

Example 3—The following example pings an IPv6 address:

```
switchxxxxxx# ping ipv6 3003::11
```

```
Pinging 3003::11 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50
```

reload

To reload the operating system, use the **reload** Privileged EXEC mode command.

Syntax

reload

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# reload
Proceed with reload? [confirm]
```

show cpu input rate

To show the current rate of input frames to CPU, use the **show cpu input rate** Privileged EXEC mode command.

Syntax

show cpu input rate

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show cpu input rate
Input Rate to CPU is 5 pps
```

show cpu utilization

To show the current CPU utilization of the switch, use the **show cpu utilization** Privileged EXEC mode command.

Syntax

show cpu utilization

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show cpu utilization
CPU utilization service is on.

CPU utilization
---------------
five seconds: 3%; one minute: 4%; five minutes: 5%
```

show memory statistics

To show the current memory utilization of the switch, use the **show memory statistics** Privileged EXEC mode command.

Syntax

show memory statistics

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show memory statistics
           total(KB)     used(KB)     free(KB)   shared(KB)   buffer(KB)
cache(KB)
--------------------+------------+------------+------------+------------+---
---------
Mem:          127392        40992        86400            0         1376
20344
-/+ buffers/cache:           19272       108120
Swap:              0            0            0
```

show services tcp-udp

To show information about the active TCP and UDP services, use the **show services tcp-udp** Privileged EXEC mode command.

Syntax

show services tcp-udp

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show services tcp-udp
Type  Local IP address             Remote IP address            Service  State
----  ---------------------------- ---------------------------- -------- --
------------
tcp   *:80                         *:*                          http     LISTEN
tcp6  *-80                         *-*                          http     LISTEN
tcp   *:443                        *:*                          https    LISTEN
tcp6  *-443                        *-*                          https    LISTEN
udp   *:546                          *:*
udp6  *-546                          *-*
udp   *:546                          *:*
udp6  *-546                          *-*
udp   *:5353                         *:*                            bonjour
udp6  *-5353                         *-*                            bonjour
```

The following table describes the significant fields shown in the example:

Field	Description
Type	Protocol type of the service.
Local IP Address	IP address and port number of the local end of the socket.

Field	Description
Remote IP Address	IP address and port number of the remote end of the socket.
Service	Name of the service.
State	State of the socket. Because there are no states in raw mode and usually no states are used in UDP, this column may be left blank.

show system languages

To show the list of supported languages, use the **show system languages** Privileged EXEC mode command.

Syntax

show system languages

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show system languages
   language Name     Unicode Name   Code    Version              MD5
------------------- -------------- ------- --------- ------------------------
 English             English        en_US             N/A
```

show tech-support

To automatically run the **show** commands to collect diagnostic information for technical support purposes, use the **show tech-support** Privileged EXEC mode command.

Syntax

show tech-support

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show tech-support

------------------ show version ------------------

Cisco Sx220 Series Switch Software, Version 1.0.0.16, RELEASE SOFTWARE
Copyright (c) 2014 by Cisco Systems, Inc.
Compiled Tue Mar 19 10:56:27 UTC 2014

ROM: Bootstrap program is Sx220 boot loader
BOOTLDR: Sx220 Boot Loader Version 1.0.0.6, RELEASE SOFTWARE
Compiled Mar 19 2014 - 10:44:25

Switchxxxxxx uptime is 2 days, 1 hours, 33 mins, 0 secs
system image is image-1

 Processor 700MHz , with 128M bytes of memory.
2 Gigabit Ethernet interfaces
48 Fast Ethernet interfaces

32M bytes of flash memory
Base MAC Address : 00:E0:4C:86:70:01
IP Address       : 192.168.1.52
Subnet Mask      : 255.255.255.0
Model Number     : SF220-48P
Serial Number    :
PID              : SF220-48P-K9-CN
VID              : V00


------------------ show flash ------------------
```

```
        File Name             File Size        Modified
------------------------ ---------------- ------------------------
 startup-config           1691             2000-01-01 08:02:16
 backup-config            1757             2000-01-01 08:04:16
 rsa2                     1679             2000-01-01 08:00:38
 dsa2                     668              2000-01-01 08:00:46
 ssl_cert                 891              2000-01-01 08:01:06
 image-1                  7075418          2013-11-19 10:56:27
 image-2                  7071043          2013-11-13 17:52:30


------------------ show username ------------------

 Priv  |  Type  |           User Name             |             Password
-------+--------+---------------------------------+--------------------------
--------
  15   | secret |                           cisco |
ZGZlYWYxMDM5MGU1NjBhZWE3NDVjY2JhNTNlMDQ0ZWQ=
  01   | secret |                          cisco2 |
ZGRhYWJmYTBhNDhkNTZmY2NhNDgyYWExZjZlNmIzNGI=


------------------ show users ------------------

   Username       Protocol          Location
--------------- ------------ ------------------------
       cisco       console      0.0.0.0


------------------ show running-config ------------------

config-file-header
switchxxxxxx
v1.0.0.16
CLI v1.0
@
!
!
!
!
username "cisco" secret encrypted
ZGZlYWYxMDM5MGU1NjBhZWE3NDVjY2JhNTNlMDQ0ZWQ=
username "cisco2" privilege user secret encrypted
ZGRhYWJmYTBhNDhkNTZmY2NhNDgyYWExZjZlNmIzNGI=
enable password 1234
!
!
!
voice vlan oui-table add 00:E0:BB 3COM
voice vlan oui-table add 00:03:6B Cisco
voice vlan oui-table add 00:E0:75 Veritel
voice vlan oui-table add 00:D0:1E Pingtel
voice vlan oui-table add 00:01:E3 Siemens
voice vlan oui-table add 00:60:B9 NEC/Philips
voice vlan oui-table add 00:0F:E2 H3C
```

```
voice vlan oui-table add 00:09:6E Avaya
!
!
!
!
spanning-tree mst configuration
 name "00:E0:4C:86:70:01"
!
!
!
!
!
!
!
!
aaa authentication enable default enable none
ip http timeout-policy 1 http-only
mac access-list extended mac1
 sequence 1 permit any any
qos advanced
qos map queue-cos 2 to 2
class-map c1 match-any
 match access-group mac1
class-map c2 match-any
 match access-group mac1
class-map c3 match-any
 match access-group mac1
!
!
!
!
!
!
!
interface gi1
!
interface gi2
!
interface gi3
!
interface gi4
!
interface gi5
!
interface gi6
!
interface gi7
!
interface gi8
!
interface gi9
!
interface gi10
!
interface gi11
```

```
!
interface gi12
!
interface gi13
!
interface gi14
!
interface gi15
!
interface gi16
!
interface gi17
!
interface gi18
!
interface gi19
!
interface gi20
!
interface gi21
!
interface gi22
!
interface gi23
!
interface gi24
!
!
!
!


------------------ show interfaces ------------------
```

show username

To show information about all administrative users, use the **show username** Privileged EXEC mode command.

Syntax

show username

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show username
 Priv   |  Type   |            User Name             |             Password
------+--------+-----------------------------+------------------------------
  15    | secret |                           cisco | Fz/1T6Qv98Ldo
```

The following table describes the significant fields shown in the example:

Field	Description
Priv	Privilege level of the user.
Type	Type of password set for the user.
User Name	Name of the user.
Password	Current password of the user.

show users

To show information about all active users, use the **show users** Privileged EXEC mode command.

Syntax

show users

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show users
Username       Protocol          Location
-------------- ------------ ----------------------
       cisco       console      0.0.0.0
       cisco        telnet      192.168.1.111
```

The following table describes the significant fields shown in the example:

Field	Description
Username	Name of the current active user.
Protocol	Interface protocol for the current active user.
Location	Location address of the current active user.

show version

To show the system version, use the **show version** Privileged EXEC mode command.

Syntax

show version

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show version
Cisco Sx220 Series Switch Software, Version 1.0.0.16, RELEASE SOFTWARE
Copyright (c) 2014 by Cisco Systems, Inc.
Compiled Wed Feb 26 16:02:49 UTC 2014

ROM: Bootstrap program is Sx220 boot loader
BOOTLDR: Sx220 Boot Loader Version , RELEASE SOFTWARE
Compiled

switchxxxxxx uptime is 1 days, 1 hours, 31 mins, 26 secs
system image is image-2

 Processor 500MHz , with 128M bytes of memory.
28 Gigabit Ethernet interfaces
0 Fast Ethernet interfaces

32M bytes of flash memory
Base MAC Address : 00:E0:4C:86:70:01
IP Address        : 192.168.1.254
Subnet Mask       : 255.255.255.0
Model Number      : SG220-28MP
Serial Number     :
PID               :
VID               : V01
```

port leds enable

To turn off the LEDs on all ports on a device, use the **no port leds enable** Global Configuration mode command.

To set the LEDs of all the ports on the device to their current operational status of the port, use the **port leds enable** command.

Syntax

port leds enable

no port leds enable

Parameters

N/A

Default Configuration

The default is **port leds enable**; that is, the LEDs of all the ports reflect their current statuses .

Command Mode

Global Configuration mode

User Guidelines

To turn off all ports LEDs on device, use the **no port leds enable** Global Configuration mode command. Use **port leds enable** to restore LEDs to current status

Example

The following example shows how to disable and enable port leds statuses:

```
switchxxxxxx(config)# no port leds enable
switchxxxxxx(config)# show port leds configuration
Port LEDs: Disabled
switchxxxxxx(config)# port leds enable
switchxxxxxx(config)# show port leds configuration
Port LEDs: Enabled
```

show port leds configuration

To display whether the LEDs of the ports are enabled or disabled, use the **show port leds configuration** EXEC mode command.

Syntax

show port leds configuration

Parameters

N/A

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

This example shows how to show port leds configuration:

```
SwitchXXXXXX# show port leds configuration
Port LEDs: Enabled
```

traceroute

To show the routes that the packets will take when traveling to their destination, use the **traceroute** Privileged EXEC mode command.

Syntax

traceroute {*ipv4-address* | *hostname*} [**max-hop** *hop-count*]

Parameters

- *ipv4-address*—IPv4 address of the destination host.
- *hostname*—Hostname of the destination host.
- **max_hop** *hop-count*—(Optional) Specifies the number of maximum hops in a region before the BPDU is discarded. (Range: 2 to 255, default : 30)

Default Usage

The default value of hop-count is 30.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# traceroute 192.168.1.55
traceroute to 192.168.1.55 (192.168.1.55), 30 hops max, 40 byte packets
 1  192.168.1.254 (192.168.1.254)  3010 ms !H  3010 ms !H  3010 ms !H
```

The following table describes the significant fields shown in the example:

Field	Description

1	Sequence number of the router in the path to the host.
192.168.1.55	IP address of the destination host.
3010 ms 3010 ms 3010 ms	Round-trip time for the probes that are sent.

The following are characters that can appear in the **traceroute** command output:

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this is output.
F	Fragmentation required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded.
S	Source route failed.
U	U Port unreachable.

38

TACACS+ Commands

show tacacs default-config

To show the default Terminal Access Controller Access-Control System Plus (TACACS+) parameters, use the **show tacacs default-config** Privileged EXEC mode command.

Syntax

show tacacs default-config

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show tacacs default-config
 Timeout|   Key
--------+---------
    20   | accounting12345
```

The following table describes the significant fields shown in the example:

Field	Description
Timeout	Default number of seconds that passes before the connection between the switch and the TACACS+ server times out.

Field	Description
Key	Default authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ server.

show tacacs

To show information for all TACACS+ servers defined on the switch, use the **show tacacs** Privileged EXEC mode command.

Syntax

show tacacs

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show tacacs
Prio | Timeout |     IP Address    |  Port  |   Key
-----+---------+-----------------+--------+----------
    2 |     10   |       10.172.11.3 |     49 | acounting1234
```

The following table describes the significant fields shown in the example:

Field	Description
Prio	Priority of the TACACS+ server, where 0 has the highest priority.
Timeout	Number of seconds that passes before the connection between the switch and the TACACS+ server times out.

Field	Description
IP Address	IP address or hostname of the TACACS+ server.
Port	TCP port number of the TACACS+ server for authentication requests. The value of zero indicates that the host is not used for authentication.
Key	Key for authenticating and encrypting the TACACS+ communications between the switch and the TACACS+ server.

tacacs-server default-param

To define the default TACACS+ parameters, use the **tacacs-server default-param** Global Configuration mode command.

Syntax

tacacs-server default-param [**key** *key-string*] [**timeout** *timeout*]

Parameters

- **key** *key-string*—(Optional) Specifies the key for authenticating and encrypting the TACACS+ communications between the switch and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0 to 128 characters)
- **timeout** *timeout*—(Optional) Specifies the number of seconds that passes before the connection between the switch and the TACACS+ server times out. (Range: 1 to 30 seconds)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

The switch can be configured to use this default key or to use a key for an individual server. If you set a default key and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

Example

The following example sets accounting12345 as the authentication and encryption key for all TACACS+ servers:

```
switchxxxxxx(config)# tacacs-server default-param key accounting12345
```

tacacs-server host

To define a TACACS+ host, use the **tacacs-server host** Global Configuration mode command.

To delete a TACACS+ host, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address* | *hostname*} [**key** *key-string*] [**port** *port-number*] [**priority** *priority*] [**timeout** *timeout*]

no tacacs-server host {*ip-address* | *hostname*}

Parameters

- *ip-address*—IP address of the TACACS+ server.
- *hostname*—Hostname of the TACACS+ server.
- **key** *key-string*—(Optional) Specifies the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "".
- **port** *port-number*—(Optional) Specifies the TCP port number through which the TACACS+ session occurs. If the port number is set to 0, the host is not used for authentication. (Range: 0 to 65535, default: 49)

- **priority** *priority*—(Optional) Specifies the priority of the TACACS+ server, where 0 is the highest priority and will be used first. If the switch cannot establish a session with the highest priority server, the switch will try the next priority server. (Range: 0 to 65535)
- **timeout** *timeout*—(Optional) Specifies the number of seconds that passes before the connection between the switch and the TACACS+ server times out. (Range: 1 to 30)

Default Configuration

No TACACS+ host is specified.

If **key-string** is not specified, the global value (set in the **tacacs-server default-param** command) is used.

If **timeout** is not specified, the global value (set in the **tacacs-server default-param** command) is used.

If a parameter was not set in one of the above commands, the default for that command is used. For example, if a timeout value was not set in the current command or in the **tacacs-server default-param** command, the default timeout set in the **tacacs-server default-param** command is used.

Command Mode

Global Configuration mode

User Guidelines

Multiple **tacacs-server host** commands can be used to specify multiple hosts.

Example

```
switchxxxxxx(config)# tacacs-server host tacassrv1 priority 20 timeout 20
```

39

Telnet and SSH Commands

crypto certificate generate

To create a self-signed certification for HTTPS, use the **crypto certificate generate** Global Configuration mode command.

Syntax

crypto certificate generate

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# crypto certificate generate
Generating a 1024 bit RSA private key
.....................................................................++++++
...........++++++
writing new private key to '/mnt/ssl_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:
```

crypto key generate

To create a public and private DSA key (DSA key pair) or a public and private RSA key (RSA key pair), use the **crypto key generate** Global Configuration mode command.

Syntax

crypto key generate {**dsa** | **rsa**}

Parameters

- **dsa**—Creates a DSA key pair.
- **rsa**—Creates a RSA key pair.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs—one public DSA key and one private DSA key. If the switch already has DSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

RSA keys are generated in pairs—one public RSA key and one private RSA key. If the switch already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the Running Configuration file. However, the keys generated by this command are saved in a private configuration (which is never displayed to the user or saved to another device).

Example

Example 1—The following example generates DSA key pair:

```
switchxxxxxx(config)# crypto key generate dsa
Replace Existing Key ? (Y/N)[N]Y
Generating a SSHv2 default DSA Key.
This may take a few minutes, depending on the key size.
```

Example 2—The following example generates RSA key pair:

```
switchxxxxxx(config)# crypto key generate rsa
Replace Existing Key ? (Y/N)[N]Y
Generating a SSHv2 default RSA Key.
This may take a few minutes, depending on the key size.
```

ip ssh server

To enable the Secure Shell (SSH) service on the switch, use the **ip ssh server** Global Configuration mode command.

To disable the SSH service on the switch, use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Parameters

N/A

Default Configuration

SSH is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The switch can be configured from a SSH server or Telnet (or both). To control the switch configuration by Telnet, use the **ip telnet server** Global Configuration mode command.

Example

```
switchxxxxxx(config)# ip ssh server
SSH daemon enabled.
```

ip telnet server

To enable the Teletype Network (Telnet) service on the switch, use the **ip telnet server** Global Configuration mode command.

To disable the Telnet service on the switch, use the **no** form of this command.

Syntax

ip telnet server

no ip telnet server

Parameters

N/A

Default Configuration

Telnet is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The switch can be configured from a SSH server or Telnet (or both). To control the switch configuration by SSH, use the **ip ssh server** Global Configuration mode command.

Example

```
switchxxxxxx(config)# ip telnet server
```

40

User Interface Commands

banner exec

To set the EXEC banner, use the **banner exec** Global Configuration mode command.

To delete the EXEC banner, use the **no** form of this command.

Syntax

banner exec *delimiter*

no banner exec

Parameters

- *delimiter*—The text message that is preceded and followed by the same single-character delimiter. The message is maximum 2000 characters long and should be typed in from a new line.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

The EXEC banner shows at the left top of the Getting Started page when users log in to the switch's web-based interface or on the command-line interface when users log in to the switch's command-line interface.

Example

The following example sets the EXEC banner, including the hostname, system contact, system location, and MAC address of the switch:

```
switchxxxxxx(config)# banner exec !
Enter TEXT message.  End with the character '!'
              ~ WELCOME ~
---------------------------------------
Host Name = $(hostname)
Bold Text = $(bold)Bold Text$(bold)
Inverse   = $(inverse)Inverse Test$(inverse)
Contact   = $(contact)
Location  = $(location)
Mac Addr  = $(mac-address)
!
```

The following table describes the variables defined in the example:

Token	Description
$(hostname)	Displays the hostname for the switch.
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the switch.

banner login

To set the login banner, use the **banner login** Global Configuration mode command.

To delete the login banner, use the **no** form of this command.

Syntax

banner login *delimiter*

no banner login

Parameters

- *delimiter*—The text message that is preceded and followed by the same single-character delimiter. The message is maximum 2000 characters long and should be typed in from a new line.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

The login banner shows on the login page when users try to access the switch's web-based interface or on the command-line interface when users try to access the switch's command-line interface.

Example

The following example sets the login banner, including the hostname, system contact, system location, and MAC address of the switch:

```
switchxxxxxx(config)# banner login !
Enter TEXT message.  End with the character '!'
~ WELCOME ~
----------------------------------------
Host Name = $(hostname)
Bold Text = $(bold)Bold Text$(bold)
Inverse   = $(inverse)Inverse Test$(inverse)
Contact   = $(contact)
Location  = $(location)
Mac Addr  = $(mac-address)
!
```

The following table describes the variables defined in the example:

Token	Description
$(hostname)	Displays the hostname for the switch.
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the switch.

configure

To enter the Global Configuration mode, use the **configure** Privileged EXEC mode.

Syntax

configure [**terminal**]

Parameters

- **terminal**—(Optional) Enters the Global Configuration mode with the keyword terminal.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# configure
switchxxxxxx(config)#
```

do

To execute an EXEC-level command from the Global Configuration mode or any configuration submode, use the **do** command.

Syntax

do *command*

Parameters

- *command*—The EXEC-level command to execute.

Command Mode

N/A

Example

The following example executes the **show vlan** Privileged EXEC mode command from the Global Configuration mode:

```
switchxxxxxx(config)# do show vlan
  VID  |     VLAN Name    |        Untagged Ports        |        Tagged Ports
       |  Type
-------+------------------+------------------------------+------------------
------------+---------
     1 |          default |           fa1-24,gi1-2,po1-8 |
    --- | Default
```

disable

To leave the Privileged EXEC mode and return to the User EXEC mode, use the **disable** Privileged EXEC mode command.

Syntax

disable [*privilege-level*]

Parameters

- *privilege-level*—(Optional) The privilege level to be reduced to. If the privilege level is left blank, the level is reduced to 1.

Default Configuration

The default privilege level is 1.

Command Mode

Privileged EXEC mode

Example

The following example returns the user to level 7:

```
switchxxxxxx# disable 7
switchxxxxxx>
```

end

To end the current configuration session and return to the Privileged EXEC mode, use the **end** command.

Syntax

end

Parameters

N/A

Default Configuration

N/A

Command Mode

N/A

Example

The following example ends the Global Configuration mode session and returns to the Privileged EXEC mode:

```
switchxxxxxx(config)# end
switchxxxxxx#
```

enable

To enter the Privileged EXEC mode, use the **enable** Privileged EXEC mode command.

Syntax

enable [*privilege-level*]

Parameters

- *privilege-level*—(Optional) The privilege level (1 or 15) to enter.

Default Configuration

The default privilege level is 15.

Command Mode

Privileged EXEC mode

Examples

The following example enters the privilege level 15:

```
switchxxxxxx> enable 15
Password:**********
switchxxxxxx#
```

exit (Configuration)

To exit any mode and bring the user to the next higher mode, use the **exit** command.

Syntax

exit

Parameters

N/A

Default Configuration

N/A

Command Mode

N/A

Example

The following example changes the configuration mode from the Interface Configuration mode to the Global Configuration mode:

```
switchxxxxxx(config-if)# exit
switchxxxxxx(config)#
```

exit (EXEC)

To close an active terminal session by logging off the switch, use the **exit** Privileged EXEC mode command.

Syntax

exit

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example closes an active terminal session:

```
switchxxxxxx# exit
```

history

To enable the history buffer and set the maximum number of user commands that are saved in the history buffer for a particular line, use the **history** Line Configuration mode command.

To disable the history buffer and restore the history buffer size to its default setting, use the **no** form of this command.

Syntax

history [**size** *number-of-commands*]

no history

Parameters

- **size** *number-of-commands*—(Optional) Specifies the number of commands that the switch records in its history buffer. (Range: 1 to 256)

Default Configuration

By default, the history buffer system is enabled.

The default command history buffer size is 128 commands.

Command Mode

Line Configuration mode

User Guidelines

This command enables the history buffer and configures the command history buffer size for a particular line. It is effective from the next time that the user logs in using the console, Telnet, or SSH.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size cannot be increased above the default size.

Example

The following example changes the command history buffer size to 100 entries for Telnet:

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history 100
```

show banner

To show information for the login and exec banners, use the **show banner** Privileged EXEC mode command.

Syntax

show banner {**login** | **exec**}

Parameters

- **login**—Displays the login banner.

- **exec**—Displays the exec banner.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show banner login
System Banner: Login
Line SSH: Enable
Line Telnet: Enable
Line Console: Enable
         ~ WELCOME ~
---------------------------------------
Host Name = $(hostname)
Bold Text = $(bold)Bold Text$(bold)
Inverse   = $(inverse)Inverse Test$(inverse)
Contact   = $(contact)
Location  = $(location)
Mac Addr  = $(mac-address)
```

show history

To show the commands entered in the current session, use the **show history** Privileged EXEC mode command.

Syntax

show history

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

The buffer includes executed and unexecuted commands. Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from the configuration modes.

Example

```
switchxxxxxx# show history
Maximum History Count: 128
------------------------------------------------------------
1. enable
2. config
3. vlan 2-10
4. exit
5. show history
```

show privilege

To show the privilege level of the current user, use the **show privilege** Privileged EXEC mode command.

Syntax

show privilege

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show privilege
```

```
Current CLI Privilege is 15
```

terminal length

To modify the terminal print length, use the **terminal length** Privileged EXEC mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

terminal length *length*

no terminal length

Parameters

- *length*—Length of rows for each print. (0 means no limit.)

Default Configuration

The default terminal length is 20.

Command Mode

Privileged EXEC mode

Example

The following example changes the terminal length to 5:

```
switchxxxxxxx# terminal length 5
switchxxxxxxx# show version
Cisco Sx220 Series Switch Software, Version 1.0.0.16, RELEASE SOFTWARE
Copyright (c) 2014 by Cisco Systems, Inc.
Compiled Wed Feb 26 16:02:49 UTC 2014

ROM: Bootstrap program is Sx220 boot loader
BOOTLDR: Sx220 Boot Loader Version , RELEASE SOFTWARE
Compiled

switchxxxxxx uptime is 1 days, 1 hours, 34 mins, 31 secs
system image is image-2

 Processor 500MHz , with 128M bytes of memory.
28 Gigabit Ethernet interfaces
0 Fast Ethernet interfaces
```

```
32M bytes of flash memory
Base MAC Address : 00:E0:4C:86:70:01
IP Address       : 192.168.1.254
Subnet Mask      : 255.255.255.0
Model Number     : SG220-28MP
Serial Number    :
PID              :
VID              : V01
```

41

Voice VLAN Commands

show voice vlan

To show the voice VLAN status for all interfaces or for a specific interface, use the **show voice vlan** Privileged EXEC mode command.

Syntax

show voice vlan [**type** {**auto** | **oui**}] [**interfaces** *interface-id*]

Parameters

- **type auto**—(Optional) Displays common and specific Auto-voice-VLAN parameters.
- **type oui**—(Optional) Displays common and specific OUI-voice-VLAN parameters.
- **interface** *interface-id*—(Optional) Specifies an Ethernet interface ID or a list of Ethernet interface IDs (Relevant only for the OUI type).

Default Configuration

If the **type** keyword is not specified, the current voice VLAN type is used.

If the *interface-id* parameter is not specified, the information for all interfaces is displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Using this command without parameters displays the parameters of the current voice VLAN type. Using this command with the type parameter displays the voice VLAN parameters relevant to the type selected.

The *interface-id* parameter is relevant only for the OUI voice VLAN type.

Examples

Example 1—The following example displays the **auto** voice VLAN parameters (this is independent of the voice VLAN state actually enabled).

```
switchxxxxxx# show voice vlan type auto
Voice VLAN ID       : 1
Voice VLAN VPT      : 5
Voice VLAN DSCP     : 46
```

Example 2—The following example displays the current voice VLAN parameters when the voice VLAN state is auto-enabled.

```
switchxxxxxx# show voice vlan
Administrate Voice VLAN state   : auto-enabled
Voice VLAN ID       : 1
Voice VLAN VPT      : 5
Voice VLAN DSCP     : 46
```

Example 3—The following example displays the voice VLAN parameters when both Auto voice VLAN and OUI are disabled.

```
switchxxxxxx# show voice vlan
Administrate Voice VLAN state   : disable
Voice VLAN ID       : 1
Voice VLAN VPT      : 5
Voice VLAN DSCP     : 46
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 6
Voice VLAN 1p Remark: disabled
```

Example 4—The following example displays the voice VLAN parameters when the voice VLAN operational state is OUI.

```
switchxxxxxx# show voice vlan
Administrate Voice VLAN state   : oui-enabled
Voice VLAN ID       : 2
Voice VLAN VPT      : 5
Voice VLAN DSCP     : 46
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 6
Voice VLAN 1p Remark: disabled
```

voice vlan enable

To enable the administrative voice VLAN on an interface, use the **voice vlan enable** Interface Configuration mode command.

To disable the administrative voice VLAN on an interface, use the **no** form of this command.

Syntax

voice vlan enable

no voice vlan enable

Default Configuration

Disabled

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# voice vlan enable
```

voice vlan aging-timeout

To set the aging timeout of the OUI voice VLAN, use the **voice vlan aging-timeout** Global Configuration mode command.

Syntax

voice vlan aging-timeout *minutes*

Parameters

- *minutes*—The time delay in minutes to remove an interface from the voice VLAN after all MAC addresses of the phones detected on the interfaces have aged out. (Range: 30 to 65536 minutes)

Default Configuration

The default aging timeout is 1440 minutes.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# voice vlan aging-timeout 500
```

voice vlan cos

To set the CoS value of the OUI voice VLAN, use the **voice vlan cos** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan cos *cos* [**remark**]

no voice vlan cos

Parameters

- *cos*—The voice VLAN CoS value. (Range: 0 to 7)
- **remark**—(Optional) The Layer 2 user priority is remarked with the CoS value.

Default Configuration

The default CoS value is 6.

The Layer 2 user priority is not remarked by default.

Command Mode

Global Configuration mode

Example

The following example sets the CoS value of the OUI voice VLAN to 7 and does not do remarking:

```
switchxxxxxx(config)# voice vlan cos 7
```

voice vlan cos mode

To set the CoS mode of the OUI voice VLAN, use the **voice vlan cos mode** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan cos mode {**src** | **all**}

no voice vlan cos mode

Parameters

- **src**—QoS attributes are applied to packets with OUIs in the source MAC address. See the **voice vlan oui-table** command for more information.
- **all**—QoS attributes are applied to packets that are classified to the voice VLAN.

Default Configuration

The default mode is **src**.

Command Mode

Global Configuration mode

Example

The following example applies QoS attributes to all voice packets:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# voice vlan cos mode all
```

voice vlan dscp

To specify the DSCP value that will be advertised by LLDP in the network policy TLV, use the **voice vlan dscp** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan dscp *dscp-value*

no voice vlan dscp

Parameters

- *dscp-value*—The DSCP value to packets received on the voice VLAN. (Range: 0 to 63)

Default Configuration

46

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# voice vlan dscp 63
```

voice vlan mode

To configure the voice VLAN mode on an interface, use the **voice vlan mode** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan mode {**auto** | **manual**}

no voice vlan mode

Parameters

- **auto**—Specifies that the port is identified as a candidate to join the voice VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as voice equipment is seen on the port, the port joins the voice VLAN as a tagged port. If the time since the last telephony MAC address was aged out of the MAC address table exceeds the voice VLAN aging time, the port is removed from the voice VLAN.
- **manual**—Specifies that the port is manually assigned to the voice VLAN.

Default Configuration

The default mode is auto.

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# voice vlan mode manual
```

voice vlan oui-table

To configure the voice VLAN OUI table, use the **voice vlan oui-table** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan oui-table {**add** *mac-address-prefix* | **remove** *mac-address-prefix*} [*description*]

no voice vlan oui-table

Parameters

- **add** *mac-address-prefix*—Adds the specified MAC address prefix to the voice VLAN OUI table.
- **remove** *mac-address-prefix*—Removes the specified MAC prefix address from the voice VLAN OUI table.

- *description*—(Optional) The description for the specified MAC address in the voice VLAN OUI table. (Length: 1 to 32 characters)

Default Configuration

The default voice VLAN OUI table is:

OUI	Description
00:e0:bb	3Com Phone
00:03:6b	Cisco Phone
00:e0:75	Veritel Polycom Phone
00:d0:1e	Pingtel Phone
00:01:e3	Siemens AG Phone
00:60:b9	NEC/Philips Phone
00:0f:e2	Huawei-3Com Phone
00:09:6e	Avaya Phone

Command Mode

Global Configuration mode

User Guidelines

The classification of a packet from VoIP equipment or phones is based on the packet's OUI in the source MAC address. OUIs are globally assigned (administered) by the IEEE.

In MAC addresses, the first three bytes contain a manufacturer ID (Organizationally Unique Identifiers (OUI)) and the last three bytes contain a unique station ID.

Because the number of IP phone manufacturers that dominate the market is limited and well known, the known OUI values are configured by default and OUIs can be added or removed by the user when required.

Example

The following example adds an entry to the voice VLAN OUI table:

```
switchxxxxxx(config)# voice vlan oui-table add 00:AA:BB experimental
```

voice vlan state

To set the type of voice VLAN that is functional on the switch or to disable the voice VLAN entirely, use the **voice vlan state** Global Configuration mode command.

Syntax

voice vlan state {**auto-enabled** | **disabled** | **oui-enabled**}

Parameters

- **auto-enabled**—Sets the voice VLAN type to Auto.
- **disabled**—Disables the voice VLAN.
- **oui-enabled**—Sets the voice VLAN type to OUI.

Default Configuration

The voice VLAN type is set to Auto.

Command Mode

Global Configuration mode

User Guidelines

By default, CDP, LLDP, and LLDP MED are enabled on the switch. All ports are members of the default VLAN (VLAN 1), which is also the default voice VLAN.

Example

```
switchxxxxxx(config)# voice vlan state auto-enabled
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# voice vlan state oui-enabled
The Voice VLAN for OUI cannot be the default VLAN
```

voice vlan id

To set a VLAN as the voice VLAN, use the **voice vlan id** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan id *VLAN-id*

no voice vlan id

Parameters

- *VLAN-id*—Identifier of the VLAN as the voice VLAN. (Range: 1 to 4094)

Default Configuration

The default voice VLAN is VLAN 1.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# vlan 104
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# voice vlan id 104
```

voice vlan vpt

To define the voice VLAN priority tag (VPT) that will be advertised by LLDP in the network policy TLV, use the **voice vlan vpt** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

voice vlan vpt *vpt-value*

no voice vlan vpt

Parameters

- *vpt-value*—The VPT value to be advertised. (Range: 0 to 7)

Default Configuration

5

Command Mode

Global Configuration mode

Example

The following example sets 7 as the voice VLAN VPT:

```
switchxxxxxx(config)# voice vlan vpt 7
```

42

VLAN Commands

name (vlan)

To set the name for a VLAN, use the **name** VLAN Configuration mode command.

To remove the name for a VLAN, use the **no** form of this command.

Syntax

name *string*

no name

Parameters

- *string*—Specifies a unique name associated with this VLAN. (Length: 1 to 32 characters)

Default Configuration

N/A

Command Mode

VLAN Configuration mode. It cannot be configured for a range of VLANs.

User Guidelines

The VLAN name must be unique.

Example

```
switchxxxxxx(config)# vlan 19
switchxxxxxx(config-if)# name Marketing
```

management-vlan

To set a VLAN as the management VLAN, use the **management-vlan** Global Configuration command.

Syntax

management-vlan vlan *vlan-id*

Parameters

- **vlan** *vlan-id*—Specifies the VLAN ID as the management VLAN.

Default Configuration

The default management VLAN is VLAN 1.

Command Mode

Global Configuration mode

Example

```
witchxxxxxx(config)# management-vlan vlan 2
```

show interfaces protected-ports

To show information for the protected ports, use the **show interfaces protected-ports** Privileged EXEC mode command.

Syntax

show interfaces protected-ports *interface-id*

Parameters

- *interface-id*—Specifies an interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show interfaces protected-ports gi11
 Port    | Protected State
-------+----------------
gi11 |enabled
```

show interfaces switchport

To show the administrative and operational status for all interfaces or a specific interface, use the **show interfaces switchport** Privileged EXEC command.

Syntax

show interfaces switchport *interface-list*

Parameters

- *interface-list*—Specifies an interface ID or a list of interface IDs. The interface can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays the command output for a trunk port:

```
switchxxxxxx# show interface switchport gi1
Port : gi1
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 1,3-4,6-7,10
```

```
Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    1                default       Untagged
    3               VLAN0003         Tagged
    4               VLAN0004         Tagged
    6               VLAN0006         Tagged
    7               VLAN0007         Tagged
   10               VLAN0010         Tagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

Example 2—The following example displays the command output for a general port:

```
switchxxxxxx# show interface switchport gi1
Port : gi1
Port Mode : General
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 10
Trunking VLANs Enabled: 1,3-4,6-7,10

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    1                default       Untagged
    3               VLAN0003       Untagged
    5               VLAN0005       Untagged
    7               VLAN0007         Tagged
    9               VLAN0009         Tagged
   10               VLAN0010         Tagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

Example 3—The following example displays the command output for a access port:

```
switchxxxxxx# show interface switchport gi1
Port : gi1
Port Mode : Access
Gvrp Status : disabled
Ingress Filtering : enabled
```

```
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 5
Trunking VLANs Enabled: 1,3-4,6-7,10

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    5               VLAN0005       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

show management-vlan

To show the management VLAN status, use the **show management-vlan** Privileged EXEC command.

Syntax

show management-vlan

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show management-vlan
    Management VLAN-ID : default(2)
```

show vlan

To show information for all VLANs or for a specific VLAN, use the **show vlan** Privileged EXEC mode command.

Syntax

show vlan [*VLAN-LIST* | **dynamic** | **static**]

show vlan *VLAN-LIST* [**interfaces** *interface-id* **membership**]

Parameters

- *VLAN-LIST*—(Optional) Displays information for a VLAN ID or a list of VLAN IDs.
- **dynamic**—(Optional) Displays information for the dynamic created VLAN.
- **static**—(Optional) Displays information for the static VLAN.
- **interfaces** *interface-id*—(Optional) Specifies an interface ID or a list of interface IDs. The interface ID can be one of these types: Ethernet port or port channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show vlan 2-5
  VID  |     VLAN Name    |    Untagged Ports       |     Tagged Ports
|  Type
------+----------------+-----------------------+-----------------------+-
--------
     2 |         VLAN0002 |                         --- |     fa1-24,gi1-2,po1-
8 | Static
     3 |         VLAN0003 |                         --- |     fa1-24,gi1-2,po1-
8 | Static
     4 |         VLAN0004 |                         --- |     fa1-24,gi1-2,po1-
8 | Static
     5 |         VLAN0005 |                         --- |     fa1-24,gi1-2,po1-
8 | Static
```

show vlan default-vlan

To show the default VLAN, use the **show vlan default-vlan** Privileged EXEC command.

Syntax

show vlan default-vlan

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show vlan default-vlan
    Default VLAN-ID : 1
```

switchport access vlan

An access interface can belong to only one VLAN. To reassign an interface to a different VLAN, use the **switchport access vlan** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

Parameters

- *vlan-id*—The VLAN ID to which the port is configured.

Default Configuration

The interface belongs to the default VLAN.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

The command automatically removes the port from its previous VLAN and adds it to a new VLAN.

Example

The following example sets gi1 as an access port and assigns it to VLAN 2 (and removes it from its previous VLAN):

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

switchport default-vlan tagged

To configure the port as a tagged port in the default VLAN, use the **switchport default-vlan tagged** Interface Configuration mode command.

To return the port to an untagged port, use the **no** form of this command.

Syntax

switchport default-vlan tagged

no switchport default-vlan tagged

Parameters

N/A

Default Configuration

If the port is a member of the default VLAN, by default, it is a member as an untagged port.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

The command adds a port to the default VLAN as a tagged port. The command is available only if the port mode is trunk or general.

When a trunk port is a member in the default VLAN as a tagged port then:

- The native VLAN cannot be the default VLAN.
- The default of the native VLAN is 4095.

NOTE If the native VLAN of a port is the default VLAN when the port is added to the default VLAN as tagged, the native VLAN is set by the system to 4095.

When a general port is a member in the default VLAN as a tagged port then:

- The PVID can be the default VLAN.
- The default PVID is the default VLAN.

NOTE The PVID is not changed when the port is added to the default VLAN as a tagged. When executing the **switchport default-vlan tagged** command, the port is added (automatically by the system) to the default VLAN when the following conditions no longer exist:

- The port is a member in a LAG.
- The port is 802.1X unauthorized.
- An IP address is defined on the port.
- The port is a destination port of port mirroring.
- An IP address is defined on the default VLAN and the port is a PVE-protected port.

The **no switchport default-vlan tagged** command removes the port from the default VLAN, and returns the default VLAN mode to untagged.

Please note the following information:

- If the native VLAN of a trunk port is 4095 when the port is removed from the default VLAN (as a tagged), the native VLAN is set by the system to the default VLAN.

- The PVID of a general port is not changed when the port is removed from the default VLAN (as a tagged). If the PVID is the default VLAN, the port is added by the system to the default VLAN as an untagged.

Example

The following example configures gi11 as a tagged port in the default VLAN:

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport default-vlan tagged
```

switchport dot1q-tunnel vlan

To set the VLAN for a port when it is in the 802.1q-tunnel mode (set by the **switchport mode** command), use the **switchport dot1q-tunnel vlan** Interface Configuration mode command.

To remove 802.1q tunnel VLAN, use the **no** form of this command.

Syntax

switchport dot1q-tunnel vlan *vlan-id*

no switchport dot1q-tunnel vlan

Parameters

- *vlan-id*—Specifies the 802.1q tunnel VLAN.

Default Configuration

The default VLAN is configured as the 802.1q tunnel VLAN.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example defines gi5 as a member of the customer VLAN 2:

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# switchport mode dot1q-tunnel
```

```
switchxxxxxx(config-if)# switchport dot1q-tunnel vlan 2
```

switchport forbidden default-vlan

To forbid a port from being added to the default VLAN, use the **switchport forbidden default-vlan** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport forbidden default-vlan

no switchport forbidden default-vlan

Parameters

N/A

Default Configuration

Membership in the default VLAN is allowed.

Command Mode

Interface and Interface Range Configuration (Ethernet, port channel) modes

User Guidelines

The command may be used at any time regardless of whether the port belongs to the default VLAN.

The **no** command does not add the port to the default VLAN. It only defines an interface as permitted to be a member of the default VLAN, and the port will be added only when the conditions are met.

Example

The following example forbids gi1 from being added to the default VLAN:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport forbidden default-vlan
```

switchport forbidden vlan

To forbid adding or removing specific VLANs to or from a port, use the **switchport forbidden vlan** Interface Configuration mode command.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- **add** *vlan-list*—Adds a list of VLANs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of VLAN IDs.
- **remove** *vlan-list*—Removes a list of VLANs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of VLAN IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example forbids adding VLANs 234 to 256 to gi7:

```
switchxxxxxx(config)# interface gi7
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport forbidden vlan add 234-256
```

switchport general acceptable-frame-type

To configure the types of packets (tagged or untagged) that are filtered (discarded) on the interface, use the **switchport general acceptable-frame-type** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport general acceptable-frame-type {**tagged-only** | **untagged-only** | **all**}

no switchport general acceptable-frame-type

Parameters

- **tagged-only**—Ignores (discards) untagged packets and priority-tagged packets.
- **untagged-only**—Ignores (discards) VLAN-tagged packets (not including priority-tagged packets)
- **all**—Does not discard packets untagged or priority-tagged packets.

Default Configuration

All frame types are accepted at ingress (all).

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example configures gi3 as a general port and discards the untagged frames at ingress:

```
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type tagged-only
```

switchport general allowed vlan

General ports can receive tagged or untagged packets. To add or remove the VLANs to or from a general port and configure whether packets on the egress are tagged or untagged, use the **switchport general allowed vlan** Interface Configuration mode command.

Syntax

switchport general allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list* }

Parameters

- **add** *vlan-list*—Adds a list of VLANs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of VLAN IDs.
- **tagged**—(Optional) The port transmits tagged packets for the VLANs. This is the default value.
- **untagged**—(Optional) The port transmits untagged packets for the VLANs.
- **remove** *vlan-list*—Removes a list of VLANs. Separate nonconsecutive VLAN IDs with a comma and no space. Use a hyphen to designate a range of VLAN IDs.

Default Configuration

The port is an untagged member in the default VLAN. Packets are transmitted as untagged.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

You can change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.

Example

The following example sets gi11 to the general mode and adds VLAN 2 to it. Packets are tagged on the egress.

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
```

switchport general ingress-filtering disable

To disable port ingress filtering (no packets are discarded at the ingress) on a general port, use the **switchport general ingress-filtering disable** Interface Configuration (Ethernet, port channel) mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Parameters

N/A

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example disables port ingress filtering on gi1 1:

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

switchport general pvid

The port VLAN ID (PVID) is the VLAN to which incoming untagged and priority-tagged frames are classified on a general port. To configure the PVID of an interface when it is in the general mode, use the **switchport general pvid** Interface Configuration (Ethernet, port channel) mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

Parameters

- *vlan-id*—The VLAN as the PVID.

Default Configuration

The default VLAN is the PVID.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Examples

Example 1—The following example configures gi2 as a general port and sets its PVID to 234:

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general pvid 234
```

Example 2—The following example adds VLAN 2 as tagged, and VLAN 100 as untagged to the general port gi14, defines VID 100 as the PVID, and then reverts to the default PVID (VID=1).

```
switchxxxxxx(config)# interface gi14
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)# switchport general allowed vlan add 100 untagged
switchxxxxxx(config-if)# switchport general pvid 100
switchxxxxxx(config-if)# no switchport general pvid
```

Example 3—The following example configures VLAN on gi14 as untagged on input and untagged on output:

```
switchxxxxxx(config)# interface gi14
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general pvid 2
```

```
switchxxxxxx(config-if)# switchport general allowed vlan add 2 untagged
```

Example 4—The following example configures VLAN on gi21 as untagged on input and tagged on output:

```
switchxxxxxx(config)# interface gi21
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general pvid 2
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
```

Example 5—The following example configures VLAN on gi11 as tagged on input and tagged on output:

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)#
```

Example 6—The following example configures VLAN on gi23 as tagged on input and untagged on output:

```
switchxxxxxx(config)# interface gi23
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)#
```

switchport mode

To configure the VLAN membership mode (access, trunk, general, or dot1q-tunnel) for a port, use the **switchport mode** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport mode {**access** | **trunk** | **general** | **dot1q-tunnel**}

no switchport mode

Parameters

- **access**—Specifies an untagged Layer 2 VLAN port.
- **trunk**—Specifies a trunking Layer 2 VLAN port.
- **general**—Specifies a fully 802.1q-supported VLAN port.
- **dot1q-tunnel**—Specifies a 802.1q tunnel port.

Default Configuration

Trunk mode

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

- When the port mode is changed, it receives the configuration corresponding to the mode.
- If the port mode is changed to access mode and the access VLAN does not exist, then the port does not belong to any VLAN.
- Trunk and general ports can be changed to access mode only if all VLANs (except for an untagged PVID) are first removed.

Example

The following example configures gi1 as an access port and assigns it to VLAN 2:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

switchport mode trunk uplink

To enable a trunk mode port as an uplink port, use the **switchport mode trunk uplink** Interface Configuration (Ethernet, port channel) mode command.

Syntax

switchport mode trunk uplink

Parameters

N/A

Default Configuration

N/A

Command Mode

Interface Configuration mode (Ethernet) mode

User Guidelines

The interface to be set as an uplink port must be in the VLAN trunk mode only.

Example

```
switchxxxxxx (config)# interface gi11
switchxxxxxx (config-if)# switchport mode trunk
switchxxxxxx (config-if)# switchport mode trunk uplink
```

switchport protected

To isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch, use the **switchport protected** Interface Configuration mode command.

To disable protection on the port, use the **no** form of this command.

Syntax

switchport protected

no switchport protected

Parameters

N/A

Default Configuration

Unprotected

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

Packets are subject to all filtering rules and Filtering Database (FDB) decisions.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport protected
```

switchport trunk allowed vlan

A trunk interface is an untagged member of a single VLAN. It may be a tagged member of one or more VLANs. To add or remove VLANs to or from a trunk port, use the **switchport trunk allowed vlan** Interface Configuration mode command.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list* | **all**}

Parameters

- **add** *vlan-list*—Adds a list of VLANs to a port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of VLAN IDs.
- **remove** *vlan-list*—Removes a list of VLANs from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of VLAN IDs.
- **all**—Adds or removes all VLANs from a port.

Default Configuration

Trunk port is an untagged member in the default VLAN and is not tagged member in any other VLANs.

Command Mode

Interface Configuration (Ethernet, port channel) mode

Example

The following example adds VLANs 2, 3, and 100 to trunk ports 1 to 13:

```
switchxxxxxx(config)# interface range gi1-13
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
```

switchport trunk native vlan

If an untagged packet arrives on a trunk port, it is directed to the port's native VLAN. To define the native VLAN for a trunk port, use the **switchport trunk native vlan** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Parameters

- *vlan-id*—The native VLAN ID.

Default Configuration

The default VLAN is the native VLAN.

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

The command adds the port as a member of the VLAN. If the port is already a member of the VLAN (not a native), it must first be removed from that VLAN.

Example

The following example defines VLAN 2 as the native VLAN for gi11.

```
switchxxxxxx(config)# interface gi11
```

```
switchxxxxxx(config-if)# switchport trunk native vlan 2
```

switchport vlan tpid

To set the Modified Tag Protocol Identifier (TPID) for an interface, use the **switchport vlan tpid** Interface Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

switchport vlan tpid {*0x8100* | *0x88A8* | *0x9100* | *0x9200*}

Parameters

- *0x8100* —The TPID is 0x8100.
- *0x88A8* —The TPID is 0x88A8.
- *0x9100* —The TPID is 0x9100.
- *0x9200* —The TPID is 0x9200.

Default Configuration

The default TPID is 0x8100.

Command Mode

Interface Configuration mode

Example

```
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# switchport vlan tpid 0x88A8
```

vlan

To create a VLAN or a list of VLANs, use the **vlan** Global Configuration mode command.

To delete the VLANs, use the **no** form of this command.

Syntax

vlan *vlan-range*

no vlan *vlan-range*

Parameters

- *vlan-range*—A list of VLANs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of VLAN IDs (range: 1 to 4094).

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

Example

The following example creates a new VLAN (VLAN 100):

```
switchxxxxxx(config)# vlan 100
switchxxxxxx(config-vlan)#
```

vlan default-vlan

To define the default VLAN, use the **vlan default-vlan** VLAN Configuration mode command.

To set the VLAN 1 as the default VLAN, use the **no** form of this command.

Syntax

vlan default-vlan *vlan-id*

no vlan default-vlan

Parameters

- *vlan-id*—Specifies the default VLAN ID.

Default Configuration

The default VLAN is VLAN 1 by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command becomes effective after the switch reboots.

Example

The following example defines the default VLAN as VLAN 2:

```
switchxxxxxx(config)# vlan default-vlan 2
```

43

Web Server Commands

ip http secure-server

To enable the HTTPS service on the switch, use the **ip http secure-server** Global Configuration mode command.

To disable the HTTPS service on the switch, use the **no** form of this command.

Syntax

ip http secure-server

no ip http secure-server

Parameters

N/A

Default Configuration

The HTTPS service is enabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip http secure-server
```

ip http server

To enable the HTTP service on the switch, use the **ip http server** Global Configuration mode command.

To disable the HTTP service on the switch, use the **no** form of this command.

Syntax

ip http server

no ip http server

Parameters

N/A

Default Configuration

The HTTP service is enabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip http server
```

ip http timeout-policy

To set the interval that the switch waits for user inputs for HTTP or HTTPS sessions before automatic logoff, use the **ip http timeout-policy** Global Configuration mode command.

To revert to its default setting, use the **no** form of this command.

Syntax

ip http timeout-policy *minutes* [**http-only** | **https-only**]

no ip http timeout-policy [**http-only** | **https-only**]

Parameters

- *minutes*—Maximum number of seconds that a connection is kept open if no data is received or the response data cannot be sent out. (Range: 0 to 86400 seconds, 0 indicates no timeout)
- **http-only**—(Optional) Specifies the timeout for HTTPS sessions only.
- **https-only**—(Optional) Specifies the timeout for HTTPS sessions only.

Default Configuration

The default timeout for HTTP and HTTPS sessions is 10 seconds.

Command Mode

Global Configuration mode

User Guidelines

To specify no timeout, enter the **ip http timeout-policy 0** command.

Example

The following example configures the HTTP timeout to 1000 seconds:

```
switchxxxxxx(config)# ip http timeout-policy 1000
```

show ip http

To show the HTTP service information, use the **show ip http** Privileged EXEC mode command.

Syntax

show ip http

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip http
```

```
     HTTP daemon : enabled
Session Timeout : 10 (minutes)
```

The following table describes the significant fields shown in the example:

Field	Description
HTTP daemon	Shows that the HTTP daemon is enabled or disabled on the switch.
Session Timeout	Timeout in minutes for HTTP sessions.

show ip https

To shows the HTTPS service information, use the **show ip https** Privileged EXEC mode command.

Syntax

show ip https

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip https
    HTTPS daemon : enabled
Session Timeout : 10 (minutes)
```

The following table describes the significant fields shown in the example:

Field	Description
HTTPS daemon	Shows that the HTTPS daemon is enabled or disabled on the switch.
Session Timeout	Timeout in minutes for HTTPS sessions.

show services tcp-udp

To show information for all open TCP or UDP sessions, use the **show services tcp-udp** Privileged EXEC mode command.

Syntax

show services tcp-udp

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show services tcp-udp
Type  Local IP address             Remote IP address            Service  State
----  ---------------------------- ---------------------------- -------- --
---
---------
tcp   *:80                         *:*                          http     LISTE
N
tcp6  *-80                         *-*                          http     LISTE
N
tcp   *:22                         *:*                          ssh      LISTE
N
tcp6  *-22                         *-*                          ssh      LISTE
N
tcp   *:23                         *:*                          telnet   LISTE
N
tcp6  *-23                         *-*                          telnet   LISTE
N
tcp   *:443                        *:*                          https    LISTE
N
tcp6  *-443                        *-*                          https    LISTE
N
tcp   192.168.1.254:23              192.168.1.107:57739           telnet
ESTAB
LISHED
tcp   192.168.1.254:80             192.168.1.107:52333          http     TIME_
WAIT
tcp   192.168.1.254:80             192.168.1.107:52335          http     TIME_
WAIT
tcp   192.168.1.254:80             192.168.1.107:52334          http     TIME_
WAIT
tcp   192.168.1.254:80             192.168.1.107:52336          http     TIME_
WAIT
```

```
tcp   192.168.1.254:80            192.168.1.107:52339          http     TIME_
WAIT
tcp   192.168.1.254:80            192.168.1.107:52358          http     TIME_
WAIT
tcp   192.168.1.254:80            192.168.1.107:52379          http     TIME_
WAIT
tcp   192.168.1.254:80            192.168.1.107:52380          http     TIME_
WAIT
tcp   192.168.1.254:80            192.168.1.107:52382          http     TIME_
WAIT
tcp   192.168.1.254:80            192.168.1.107:52389          http     TIME_
WAIT
tcp   192.168.1.254:80            192.168.1.107:52388          http     TIME_
WAIT
tcp    192.168.1.254:23             192.168.1.107:52381          telnet
ESTAB
LISHED
udp    *:161                      *:*                          snmp
udp6   *-161                      *-*                          snmp
```

The following table describes the significant fields shown in the example:

Field	Description
Type	Protocol type of the service.
Local IP Address	IP address and port number of the local end of the socket.
Remote IP Address	IP address and port number of the remote end of the socket.
Service	Name of the service.

Field	Description
State	State of the socket. Because there are no states in raw mode and usually no states used in UDP, this column may be left blank. Normally this can be one of several values: ▪ ESTABLISHED—The socket has an established connection. ▪ SYN_SENT—The socket is actively attempting to establish a connection. ▪ SYN_RECV—A connection request has been received from the network. ▪ FIN_WAIT1—The socket is closed, and the connection is shutting down. ▪ FIN_WAIT2—The connection is closed, and the socket is waiting for a shutdown from the remote end. ▪ TIME_WAIT—The socket is waiting after close to handle packets still in the network. ▪ CLOSED—The socket is not being used. ▪ CLOSE_WAIT—The remote end has shut down, waiting for the socket to close. ▪ LAST_ACK—The remote end has shut down, and the socket is closed. Waiting for acknowledgment. ▪ LISTEN—The socket is listening for incoming connections. Such sockets are not included in the output unless you specify the --listening (-l) or --all (-a) option. ▪ CLOSING—Both sockets are shut down but we still do not have all our data sent. ▪ UNKNOWN—The state of the socket is unknown.

A

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco 220 Series Smart Switches.

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport
Cisco Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco products. No login is required.
Cisco Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Documentation	
Cisco 220 Series	www.cisco.com/go/220switches
Warranty Information	www.cisco.com/go/warranty
Regulatory Compliance and Safety Information	www.cisco.com/en/US/docs/switches/lan/csb_switching_general/rcsi/Switch_ClassA_RCSI.pdf
Cisco Small Business	
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb