Cisco Small Business 300 Series Managed Switches
Command Line Interface Guide Release 1.3

CLI GUIDE
Table of Contents

1 Introduction.................................................................................................................. 21

2 User Interface Commands .......................................................................................... 36
   enable ..................................................................................................................... 36
   disable .................................................................................................................... 37
   login ....................................................................................................................... 37
   configure ............................................................................................................. 38
   exit (Configuration) ............................................................................................. 39
   exit (EXEC) ......................................................................................................... 39
   end ......................................................................................................................... 40
   help ....................................................................................................................... 41
   history ................................................................................................................... 42
   history size ........................................................................................................... 43
   terminal history .................................................................................................... 44
   terminal history size ............................................................................................ 44
   terminal datadump ................................................................................................ 45
   terminal width ....................................................................................................... 46
   terminal prompt ..................................................................................................... 47
   show history ......................................................................................................... 48
   show privilege ....................................................................................................... 49
   do ......................................................................................................................... 49
   banner login ........................................................................................................ 50
   show banner ........................................................................................................ 52

3 Macro Commands ...................................................................................................... 54
   macro name .......................................................................................................... 54
   macro ..................................................................................................................... 57
   macro description ................................................................................................. 59
   macro global ......................................................................................................... 61
   macro global description ..................................................................................... 63
   show parser macro ............................................................................................... 64

4 RSA and Certificate Commands .................................................................................. 67
   crypto key generate dsa ....................................................................................... 68
   crypto key generate rsa ....................................................................................... 69
   crypto key import ................................................................................................. 70
   show crypto key .................................................................................................... 73
   crypto certificate generate .................................................................................... 74
   crypto certificate request ...................................................................................... 75
   crypto certificate import ....................................................................................... 77
   show crypto certificate .......................................................................................... 82

5 System Management Commands ............................................................................... 86
   ping ....................................................................................................................... 86
   traceroute ............................................................................................................. 89
6 SSH Client Commands ............................................................................ 120

   ip ssh-client authentication ............................................................. 120
   ip ssh-client change server password ............................................. 121
   ip ssh-client key .............................................................................. 122
   ip ssh-client password .................................................................. 125
   ip ssh-client server authentication .................................................. 126
   ip ssh-client server fingerprint ....................................................... 127
   ip ssh-client username .................................................................. 128
   show ip ssh-client ......................................................................... 129
   show ip ssh-client server ............................................................... 132

7 Clock Commands .................................................................................... 134

   clock set ......................................................................................... 134
   clock source .................................................................................. 134
   clock timezone .............................................................................. 135
   clock summer-time ....................................................................... 136
   clock dhcp timezone ..................................................................... 138
   sntp authentication-key ................................................................ 139
   sntp authenticate ......................................................................... 140
   sntp trusted-key ............................................................................ 141
**Contents**

- sntp broadcast client enable ................................................................. 142
- sntp anycast client enable ................................................................. 143
- sntp client enable ............................................................................. 144
- sntp client enable (Interface) ............................................................. 145
- sntp unicast client enable ................................................................. 146
- sntp unicast client poll ..................................................................... 146
- sntp server ......................................................................................... 147
- show clock ......................................................................................... 148
- show sntp configuration .................................................................... 149
- show sntp status ............................................................................... 150

8 **DNS Client Commands.................................................................. 153**
- clear host ......................................................................................... 153
- ip domain lookup ............................................................................. 154
- ip domain name .............................................................................. 154
- ip domain polling-interval ............................................................... 155
- ip domain retry ............................................................................... 156
- ip domain timeout .......................................................................... 157
- ip host .............................................................................................. 158
- ip name-server ................................................................................. 159
- show hosts ......................................................................................... 160

9 **Configuration and Image File Commands.................................. 163**
- copy ................................................................................................. 163
- write ................................................................................................. 170
- delete ............................................................................................... 170
- dir .................................................................................................... 171
- more ............................................................................................... 173
- boot system ..................................................................................... 174
- rename ............................................................................................ 175
- show bootvar .................................................................................. 176
- show running-config ....................................................................... 177
- show startup-config ....................................................................... 180
- service mirror-configuration ........................................................... 182
- show mirror-configuration service .................................................. 183

10 **Auto-Configuration................................................................... 185**
- boot host auto-config ...................................................................... 185
- show boot ........................................................................................ 186
- ip dhcp tftp-server ip address ......................................................... 187
- ip dhcp tftp-server file ................................................................... 187
- show ip dhcp tftp-server .................................................................. 188

11 **Management ACL Commands.............................................. 190**
- management access-list .................................................................. 190
- permit (Management) ...................................................................... 191
- deny (Management) ........................................................................ 192
- management access-class ............................................................... 194
show management access-list ................................................................. 194
show management access-class .............................................................. 195

12 Network Management Protocol (SNMP) Commands ......................... 197
   snmp-server server ................................................................. 197
   snmp-server community ........................................................... 197
   snmp-server community-group ...................................................... 199
   snmp-server view ................................................................. 200
   show snmp views ........................................................................ 202
   snmp-server group ..................................................................... 203
   show snmp groups ...................................................................... 204
   snmp-server user ....................................................................... 205
   show snmp users ....................................................................... 208
   snmp-server filter ...................................................................... 210
   show snmp filters ....................................................................... 211
   snmp-server host ....................................................................... 212
   snmp-server engineID remote ......................................................... 214
   snmp-server engineID local .......................................................... 215
   show snmp engineID ................................................................... 216
   snmp-server enable traps ............................................................... 217
   snmp-server trap authentication ...................................................... 218
   snmp-server contact ................................................................... 218
   snmp-server location ................................................................... 219
   snmp-server set ......................................................................... 220
   show snmp ............................................................................... 221

13 Web Server Commands ................................................................. 223
   ip http server ........................................................................ 223
   ip http port .............................................................................. 223
   ip http timeout-policy ................................................................. 224
   ip http secure-server ................................................................. 225
   ip https certificate .................................................................... 226
   show ip http ............................................................................ 227
   show ip https ........................................................................... 227

14 Telnet, Secure Shell (SSH) and Secure Login (Slogin) Commands ...... 229
   ip telnet server ........................................................................ 229
   ip ssh server ............................................................................ 230
   ip ssh port ............................................................................... 230
   ip ssh pubkey-auth .................................................................... 231
   ip ssh password-auth ................................................................. 232
   crypto key pubkey-chain ssh ....................................................... 233
   user-key ............................................................................... 235
   key-string ............................................................................... 236
   show ip ssh ............................................................................. 237
   show crypto key pubkey-chain ssh ............................................. 238

15 Line Commands ............................................................................. 240
16 Bonjour Commands .................................................................................. 245
- bonjour enable .......................................................... 245
- bonjour interface range ........................................... 245
- show bonjour .......................................................... 246

17 Authentication, Authorization and Accounting (AAA) Commands ....... 248
- aaa authentication login ........................................... 248
- aaa authentication enable ........................................ 249
- login authentication .................................................. 251
- enable authentication ............................................... 252
- ip http authentication ............................................... 253
- show authentication methods .................................. 255
- password .............................................................. 256
- enable password ..................................................... 256
- service password-recovery .................................... 258
- username .............................................................. 259
- show users accounts ............................................... 260
- aaa accounting login .............................................. 261
- aaa accounting dot1x ............................................... 263
- show accounting ..................................................... 265
- passwords complexity enable .................................. 266
- passwords complexity <attributes> .......................... 268
- passwords aging .................................................... 269
- show passwords configuration ................................ 270

18 RADIUS Commands ............................................................................. 272
- radius-server host .................................................... 272
- radius-server key .................................................... 274
- radius-server retransmit ......................................... 275
- radius-server source-ip ......................................... 276
- radius-server source-ipv6 ....................................... 277
- radius-server timeout ............................................ 277
- radius-server deadtime .......................................... 278
- show radius-servers ................................................. 279
- show radius-servers key ........................................ 280

19 TACACS+ Commands ......................................................................... 281
- tacacs-server host .................................................... 281
- tacacs-server key .................................................... 282
- tacacs-server timeout .......................................... 283
- tacacs-server source-ip ....................................... 284
- tacacs-server source-ipv6 ..................................... 285
20 Syslog Commands

- logging on .................................................. 288
- logging host ................................................. 289
- logging console .............................................. 290
- logging buffered ............................................ 291
- clear logging ............................................... 292
- logging file .................................................. 292
- clear logging file ........................................... 293
- aaa logging .................................................. 294
- file-system logging ........................................ 295
- logging aggregation on ..................................... 295
- logging aggregation aging-time ......................... 296
- logging origin-id .......................................... 297
- show logging ............................................... 298
- show logging file .......................................... 299
- show syslog-servers ........................................ 300

21 Remote Network Monitoring (RMON) Commands

- show rmon statistics ....................................... 302
- rmon collection stats ...................................... 304
- show rmon collection stats ............................... 305
- show rmon history ......................................... 306
- rmon alarm .................................................. 309
- show rmon alarm-table ................................... 311
- show rmon alarm ........................................... 312
- rmon event .................................................. 314
- show rmon events .......................................... 315
- show rmon log ............................................. 316
- rmon table-size ............................................ 317

22 802.1X Commands

- aaa authentication dot1x .................................. 319
- dot1x system-auth-control ............................... 320
- dot1x port-control ......................................... 320
- dot1x reauthentication .................................... 322
- dot1x timeout reauth-period ............................ 322
- dot1x re-authenticate ...................................... 323
- dot1x timeout quiet-period .............................. 324
- dot1x timeout tx-period .................................. 325
- dot1x max-req ............................................. 326
- dot1x timeout supp-timeout ............................. 327
- dot1x timeout server-timeout ......................... 328
- show dot1x ................................................... 329
- show dot1x users .......................................... 332
- show dot1x statistics ...................................... 333
clear dot1x statistics ................................................................. 335
dot1x host-mode ................................................................. 336
dot1x auth-not-req .............................................................. 337
dot1x violation-mode ......................................................... 338
dot1x guest-vlan .............................................................. 339
dot1x guest-vlan timeout ................................................... 340
dot1x guest-vlan enable ..................................................... 341
dot1x mac-authentication ................................................... 341
dot1x radius-attributes vlan .............................................. 342
show dot1x advanced ......................................................... 344

23 Ethernet Configuration Commands ......................................... 346
interface ................................................................. 346
interface range ........................................................... 347
shutdown ................................................................. 347
operation time ........................................................... 348
description .............................................................. 349
speed ................................................................. 350
duplex ................................................................. 351
negotiation ............................................................. 352
flowcontrol ............................................................ 353
mdix ................................................................. 354
back-pressure .......................................................... 355
port jumbo-frame ......................................................... 355
clear counters .......................................................... 356
set interface active ....................................................... 357
show interfaces configuration ........................................... 357
show interfaces status .................................................... 358
show interfaces advertise .................................................. 359
show interfaces description ............................................... 361
show interfaces counters .................................................. 362
show ports jumbo-frame ..................................................... 365
show errdisable interfaces .................................................. 366
storm-control broadcast enable ............................................ 366
storm-control broadcast level ............................................... 367
storm-control include-multicast ............................................ 368
show storm-control ......................................................... 369

24 PHY Diagnostics Commands ............................................... 370
test cable-diagnostics tdr .................................................. 370
show cable-diagnostics tdr .................................................. 371
show cable-diagnostics cable-length ..................................... 372
show fiber-ports optical-transceiver ..................................... 373

25 Power over Ethernet (PoE) Commands .................................... 375
power inline .......................................................... 375
power inline powered-device ............................................. 376
power inline priority ....................................................... 377
26 EEE Commands ................................................................. 385
  eee enable (global) ............................................................ 385
  eee enable (interface) ......................................................... 385
  eee lldp enable ................................................................. 386
  show eee .......................................................... 387

27 Green Ethernet .............................................................. 393
  green-ethernet energy-detect (global) ................................. 393
  green-ethernet energy-detect (interface) .............................. 393
  green-ethernet short-reach (global) ..................................... 394
  green-ethernet short-reach (interface) ................................. 395
  green-ethernet power-meter reset ....................................... 396
  show green-ethernet ...................................................... 396

28 Port Channel Commands .................................................. 399
  channel-group .............................................................. 399
  port-channel load-balance ................................................ 400
  show interfaces port-channel ............................................ 400

29 Address Table Commands ............................................... 403
  bridge multicast filtering .................................................. 403
  bridge multicast mode ...................................................... 404
  bridge multicast address .................................................. 406
  bridge multicast forbidden address .................................... 407
  bridge multicast ip-address ............................................... 408
  bridge multicast forbidden ip-address ................................ 410
  bridge multicast source group ........................................... 411
  bridge multicast forbidden source group ............................. 412
  bridge multicast ipv6 mode ............................................... 413
  bridge multicast ipv6 ip-address ........................................ 415
  bridge multicast ipv6 forbidden ip-address ........................ 416
  bridge multicast ipv6 source group ..................................... 418
  bridge multicast ipv6 forbidden source group ....................... 419
  bridge multicast unregistered .......................................... 420
  bridge multicast forward-all ............................................ 421
  bridge multicast forbidden forward-all ............................... 422
  bridge unicast unknown ................................................... 423
  mac address-table static .................................................. 424
  clear mac address-table .................................................... 426
  show bridge unicast unknown ............................................ 427
  mac address-table aging-time ............................................ 428
32 Virtual Local Area Network (VLAN) Commands .......................................................... 487
- vlan database ............................................................................................................... 487
- vlan ............................................................................................................................ 488
- show vlan ..................................................................................................................... 488
- default-vlan vlan ........................................................................................................... 491
- show default-vlan-membership ....................................................................................... 492
- interface vlan ................................................................................................................ 492
- interface range vlan ..................................................................................................... 493
- name ............................................................................................................................. 494
- switchport protected-port ............................................................................................ 495
- show interfaces protected-ports .................................................................................. 496
- switchport mode .......................................................................................................... 496
- switchport access vlan ................................................................................................. 498
- switchport trunk allowed vlan ..................................................................................... 500
- switchport trunk native vlan ........................................................................................ 501
- switchport general allowed vlan .................................................................................. 503
- switchport general pvid ............................................................................................... 504
- switchport general ingress-filtering disable ............................................................... 506
- switchport general acceptable-frame-type ............................................................... 507
- switchport customer vlan ........................................................................................... 508
- map mac macs-group .................................................................................................... 509
- switchport general map macs-group vlan ................................................................. 510
- show vlan macs-groups .............................................................................................. 511
- switchport forbidden default-vlan .............................................................................. 512
- switchport forbidden vlan .......................................................................................... 513
- switchport default-vlan tagged ................................................................................... 514
- show interfaces switchport ......................................................................................... 516
- ip internal-usage-vlan ................................................................................................. 518
- show vlan internal usage .............................................................................................. 519
- switchport access multicast-tv vlan ............................................................................ 520
- switchport customer multicast-tv vlan ........................................................................ 521
- show vlan multicast-tv ................................................................................................ 522
- vlan prohibit-internal-usage ......................................................................................... 523
- show vlan internal usage .............................................................................................. 524

33 Voice VLAN Commands .............................................................................................. 526
- voice vlan state ............................................................................................................ 526
- voice vlan refresh ........................................................................................................ 528
- voice vlan id ................................................................................................................ 530
- voice vlan vpt ............................................................................................................. 531
- voice vlan dscp .......................................................................................................... 532
- voice vlan oui-table ..................................................................................................... 533
- voice vlan cos mode ................................................................................................... 534
34  SSD Commands  ................................................................. 544
    ssd config ................................................................. 544
    passphrase .............................................................. 544
    ssd rule ................................................................. 545
    show SSD ............................................................... 548
    ssd session read ...................................................... 549
    show ssd session ...................................................... 550
    ssd file passphrase control ...................................... 551
    ssd file integrity control ......................................... 552

35  Smartport Commands ................................................... 554
    macro auto (Global) .................................................. 554
    macro auto smartport (Interface) ............................... 555
    macro auto trunk refresh ......................................... 556
    macro auto resume .................................................. 557
    macro auto persistent ............................................. 558
    macro auto smartport type ....................................... 559
    macro auto processing cdp ....................................... 561
    macro auto processing lldp ...................................... 562
    macro auto processing type ...................................... 563
    macro auto user smartport macro ............................... 564
    macro auto built-in parameters ................................ 565
    show macro auto processing ...................................... 566
    show macro auto smart-macros .................................. 567
    show macro auto ports ............................................ 569
    smartport switchport trunk allowed vlan ................... 571
    smartport switchport trunk native vlan ..................... 572
    smartport storm-control broadcast enable ................... 572
    smartport storm-control broadcast level ..................... 573
    smartport storm-control include-multicast ................. 574

36  CDP Commands .......................................................... 576
    cdp run ............................................................... 576
    cdp enable .......................................................... 577
    cdp pdu .............................................................. 577
    cdp advertise-v2 .................................................... 578
    cdp appliance-tlv enable .......................................... 579
    cdp mandatory-tlvs validation .................................. 580
    cdp source-interface ............................................... 581
    cdp log mismatch duplex ......................................... 582
    cdp log mismatch voip ............................................. 582
    cdp log mismatch native .......................................... 583

voice vlan cos .............................................................. 535
voice vlan aging-timeout .............................................. 536
voice vlan enable ......................................................... 536
show voice vlan .......................................................... 537
show voice vlan local ................................................... 541
37 Link Layer Discovery Protocol (LLDP) Commands ........................................ 601
   lldp run ................................................................. 601
   lldp transmit ......................................................... 601
   lldp receive .......................................................... 602
   lldp timer ............................................................. 603
   lldp hold-multiplier ................................................ 604
   lldp reinit .............................................................. 605
   lldp tx-delay .......................................................... 605
   lldp optional-tlv .................................................... 606
   lldp optional-tlv 802.1 .............................................. 607
   lldp management-address ........................................ 608
   lldp notifications ................................................... 610
   lldp notifications interval ........................................ 610
   lldp llpdpu ........................................................... 611
   lldp med .............................................................. 612
   lldp med notifications topology-change ....................... 613
   lldp med fast-start repeat-count ................................ 614
   lldp med network-policy (global) ............................... 615
   lldp med network-policy (interface) ........................... 616
   lldp med network-policy voice auto ............................ 617
   clear lldp table ..................................................... 618
   lldp med location ................................................... 619
   show lldp configuration ........................................... 620
   show lldp med configuration ..................................... 623
   show lldp local tlv-overloading .................................. 624
   show lldp local ....................................................... 625
   show lldp statistics ............................................... 627
   show lldp neighbors ................................................ 629

38 IGMP Snooping Commands ......................................................... 635
   ip igmp snooping (Global) ......................................... 635
   ip igmp snooping vlan ............................................. 635
   ip igmp snooping vlan mrouter .................................. 636
   ip igmp snooping vlan mrouter interface ....................... 637
   ip igmp snooping vlan forbidden mrouter ....................... 638
Contents

40 Link Aggregation Control Protocol (LACP) Commands ........................................ 668
  lACP system-priority .............................................. 668
  lACP port-priority .............................................. 668
  lACP timeout ..................................................... 669
  show lACP ....................................................... 670
  show lACP port-channel ......................................... 672

41 GARP VLAN Registration Protocol (GVRP) Commands .................................. 674
  gVRP enable (Global) ........................................... 674
  gVRP enable (Interface) ....................................... 674
  gVRP vlan-creation-forbid .................................... 675
  gVRP registration-forbid ....................................... 676
  clear gVRP statistics ............................................ 676

39 IPv6 MLD Snooping Commands ....................................................................... 654
  ipv6 mld snooping (Global) ...................................... 654
  ipv6 mld snooping vlan ......................................... 654
  ipv6 mld robustness ............................................. 655
  ipv6 mld snooping vlan mrouter ................................ 656
  ipv6 mld snooping vlan mrouter ................................ 657
  ipv6 mld snooping vlan forbidden mrouter .................. 658
  ipv6 mld snooping vlan static .................................. 659
  ipv6 mld query-interval ........................................ 660
  ipv6 mld query-max-response-time ............................ 661
  ipv6 mld last-member-query-count ............................. 661
  ipv6 mld last-member-query-interval .......................... 662
  ipv6 mld snooping vlan immediate-leave ....................... 663
  show ipv6 mld snooping mrouter ................................ 664
  show ipv6 mld snooping interface ............................... 665
  show ipv6 mld snooping groups ................................ 666

ip igmp snooping vlan static ............................................. 639
ip igmp snooping vlan multicast-tv ................................ 640
ip igmp snooping map cpe vlan ...................................... 641
ip igmp snooping vlan querier ...................................... 642
ip igmp snooping vlan querier address ........................... 643
ip igmp snooping vlan querier version ............................. 643
ip igmp robustness .................................................. 644
ip igmp query-interval ............................................. 645
ip igmp query-max-response-time .................................. 646
ip igmp last-member-query-count .................................. 647
ip igmp last-member-query-interval ................................ 647
ip igmp snooping vlan immediate-leave ........................... 648
show ip igmp snooping mrouter .................................... 649
show ip igmp snooping interface .................................... 650
show ip igmp snooping groups ....................................... 651
show ip igmp snooping multicast-tv ............................... 652
show ip igmp snooping cpe vlans ................................... 653
42 DHCP Snooping and ARP Inspection Commands ........................................ 681

43 IP Addressing Commands ...................................................................... 708
deny (IP) ................................................................. 773
ipv6 access-list (IPv6 extended) ........................................ 776
permit (IPv6) ............................................................ 777
deny (IPv6) ............................................................. 779
mac access-list ....................................................... 781
permit (MAC) ........................................................... 782
deny (MAC) .............................................................. 784
service-acl input ....................................................... 785
time-range ............................................................. 786
absolute ................................................................. 788
periodic ................................................................. 789
show time-range ....................................................... 790
show access-lists .................................................... 791
show interfaces access-lists ........................................ 792

49 Quality of Service (QoS) Commands ........................................ 794
qos ................................................................. 794
qos advanced-mode trust ........................................... 795
show qos ............................................................. 796
class-map .............................................................. 797
show class-map ....................................................... 799
match ................................................................. 799
policy-map ............................................................. 800
class ................................................................. 801
show policy-map ..................................................... 802
trust ................................................................. 803
set ................................................................. 805
police ................................................................. 806
service-policy ....................................................... 807
qos aggregate-policer ............................................... 808
show qos aggregate-policer ........................................ 810
police aggregate ..................................................... 810
wrr-queue cos-map ................................................ 811
wrr-queue bandwidth .............................................. 813
priority-queue out num-of-queues ................................ 814
traffic-shape ....................................................... 815
traffic-shape queue ................................................ 816
rate-limit (Ethernet) ............................................... 817
rate-limit (VLAN) .................................................... 818
qos wrr-queue wrtd ............................................... 819
show qos wrr-queue wrtd ......................................... 819
show qos interface .................................................. 820
wrr-queue ........................................................... 823
qos wrr-queue threshold .......................................... 824
qos map policed-dscp ............................................ 825
qos map dscp-queue ............................................... 826
qos map dscp-dp .................................................... 827
50 Denial of Service (DoS) Commands ............................................................. 839
  security-suite enable .................................................................................... 839
  security-suite dos protect .............................................................. 841
  security-suite dos syn-attack ............................................................ 842
  security-suite deny martian-addresses .................................................... 843
  security-suite deny syn ............................................................................. 845
  security-suite deny icmp ........................................................................... 846
  security-suite deny fragmented ............................................................. 848
  show security-suite configuration ........................................................ 849
  security-suite deny syn-fin ................................................................... 850
  security-suite syn protection mode ......................................................... 851
  security-suite syn protection threshold ............................................... 852
  security-suite syn protection recovery ................................................. 853
  show security-suite syn protection ....................................................... 853

51 Router Resources Commands ................................................................. 855
  system router resources ........................................................................... 855
  show system router resources ............................................................ 857

52 DHCPv6 Commands ................................................................................. 859
  ipv6 dhcp client stateless ............................................................... 859
  clear ipv6 dhcp client .......................................................................... 860
  ipv6 dhcp client information refresh .................................................. 861
  ipv6 dhcp client information refresh minimum .................................. 862
  ipv6 dhcp duid-en ................................................................................. 863
  ipv6 dhcp relay destination (Global) ....................................................... 864
  ipv6 dhcp relay destination (Interface) ................................................ 866
  show ipv6 dhcp ....................................................................................... 869
  show ipv6 dhcp interface ................................................................. 871

53 DHCP Server Commands ....................................................................... 874
  ip dhcp server ....................................................................................... 874
  ip dhcp pool host .................................................................................. 874
  ip dhcp pool network ............................................................................ 875
  address (DHCP Host) ............................................................................. 876
  address (DHCP Network) ............................................................... 877
lease ................................................................. 878
client-name ....................................................... 879
default-router ..................................................... 880
dns-server ......................................................... 880
domain-name ....................................................... 881
netbios-name-server ........................................... 882
netbios-node-type ............................................... 882
next-server ....................................................... 883
next-server-name ............................................... 884
bootfile ............................................................ 885
time-server ....................................................... 885
option .............................................................. 886
ip dhcp excluded-address ....................................... 888
clear ip dhcp binding ............................................ 888
show ip dhcp ....................................................... 889
show ip dhcp excluded-addresses ............................. 890
show ip dhcp pool host .......................................... 890
show ip dhcp pool network ..................................... 892
show ip dhcp binding ............................................ 893
show ip dhcp server statistics ................................ 895
show ip dhcp allocated .......................................... 896
show ip dhcp declined ........................................... 897
show ip dhcp expired ............................................ 898
show ip dhcp pre-allocated .................................... 899
Introduction

This section describes how to use the Command Line Interface (CLI). It contains the following topics:

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

Overview

The CLI is divided into various command modes. Each mode includes a group of commands. These modes are described in CLI Command Modes.

Users are assigned privilege levels. Each user privilege level can access specific CLI modes. User levels are described in the section below.

User (Privilege) Levels

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

- **Level 1** — Users with this level can only run User EXEC mode commands. Users at this level cannot access the web GUI or commands in the Privileged EXEC mode.

- **Level 7** — Users with this level can run commands in the User EXEC mode and a subset of commands in the Privileged EXEC mode. Users at this level cannot access the web GUI.
• **Level 15** — Users with this level can run all commands. Only users at this level can access the web GUI.

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 level 7, level 1 to 15, or level 7 to level 15.

The passwords for each level are set (by an administrator) using the following command:

```
enable password [level privilege-level] {password | encrypted encrypted-password}
```

Using these passwords, you can raise your user level by entering the command: `enable` and the password for level 7 or 15. You can go from level 1 to level 7 or directly to 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 it a user level, use the `username` command. Only users with command level 15, can create users at this level.

1. **Example 1**—Create passwords for level 7 and 15 (by the administrator):

```
switchxxxxxx#configure
switchxxxxxx<config># enable password level 7 level7@abc
switchxxxxxx<config># enable password level 15 level15@abc
switchxxxxxx<config>#
```

**Example 2**—Create a user with user level 1:

```
switchxxxxxx#configure
switchxxxxxx<config> username john password john1234 privilege 1
switchxxxxxx<config>
```
Example 3— Switch between Level 1 to Level 15. The user must know the password:

```
switchxxxxxx#
switchxxxxxx# enable
Enter Password: ****** (this is the password for level 15 - level15@abc)
switchxxxxxx#
```

NOTE If authentication of passwords is performed on RADIUS or TACACS+ servers, the passwords assigned to user level 7 and user level 15 must be configured on the external server and associated with the $enable7$ and $enable15$ user names, respectively. See the Authentication, Authorization and Accounting (AAA) Commands chapter for details.

**CLI Command Modes**

The CLI is divided into four command modes. The command modes are (in the order in which they are accessed):

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode
- Interface Configuration mode

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 User (Privilege) Levels.

**User EXEC Mode**

Users with level 1 initially log into User EXEC mode. 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 host name followed by a #. The default host name is switchxxxxxx where xxxxxx is the last six digits of the device’s MAC address, as shown below

switchxxxxxx#

The default host name can be changed via the hostname command in Global Configuration mode.

**Privileged EXEC Mode**

A user with level 7 or 15 automatically logs into Privileged EXEC mode.

Users with level 1 can enter 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 commands that configure features at the system level, as opposed to the interface level.

Only users with command level of 7 or 15 can access this mode.

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

switchxxxxxx(config)#

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

- exit
- end
- Ctrl+Z
The following example shows how to access Global Configuration mode and return to Privileged EXEC mode:

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

**Interface or Line Configuration Modes**

Various submodes may be entered from Global Configuration mode. These submodes enable performing commands on a group of interfaces or lines.

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

The following example enters Interface Configuration mode for ports gi1-5 and then sets their speed:

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# interface range gi1-5
switchxxxxxx(config-if)# speed 10
switchxxxxxx(config-if)# exit
switchxxxxxx(config)#
```

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

The following submodes are available:

- **Interface** — Contains commands that configure a specific interface (port, VLAN, port channel, or tunnel) or range of interfaces. The Global Configuration mode command interface is used to enter the Interface
Configuration mode. The **interface** Global Configuration command is used to enter this mode.

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

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

- **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 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.

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

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

## Accessing the CLI

The CLI 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,

  —or—
• 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 access is via 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.

• There is an IP path such that the computer and the switch can reach each other.

### Using HyperTerminal over the Console Interface

**NOTE**  When using HyperTerminal with Microsoft® Windows® 2000, ensure that Windows® 2000 Service Pack 2 or later is installed on your computer. The arrow keys will not function properly using HyperTerminal's VT100 emulation in Windows® 2000 prior to Service Pack 2. For information on Windows® 2000 service packs, go to www.microsoft.com.

The switch’s RS-232 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 switch are connected, run a terminal application to access the CLI.

To access the CLI using the HyperTerminal application, perform the following steps:

**STEP 1**  Click the Start button.

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

**Figure 1**  Start > 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 to communicate with the switch. Select COM1 or COM2.

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

STEP 6 When the CLI appears, enter `cisco` at the **User Name** prompt and press **Enter**.

The `switchxxxxxx#` prompt is displayed. You can now enter CLI commands to manage the switch. For detailed information on CLI commands, refer to the appropriate chapter(s) of this reference guide.

---

### Using Telnet over an Ethernet Interface

Telnet provides a method of connecting to the CLI 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.

**Figure 2**  **Start > All Programs > Accessories > Command Prompt**

STEP 2 At the prompt, enter `telnet 1<IP address of switch>`, then press **Enter**.

**Figure 3**  **Command Prompt**

STEP 3 The CLI prompt is displayed.
CLI Command Conventions

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>In a command line, square brackets indicate an optional entry.</td>
</tr>
<tr>
<td>{ }</td>
<td>In a command line, curly brackets indicate a selection of compulsory parameters separated the</td>
</tr>
<tr>
<td>parameter</td>
<td>Italic text indicates a parameter.</td>
</tr>
<tr>
<td>press key</td>
<td>Names of keys to be pressed are shown in <strong>bold</strong>.</td>
</tr>
<tr>
<td>Ctrl+F4</td>
<td>Keys separated by the + character are to be pressed simultaneously on the keyboard</td>
</tr>
<tr>
<td>Screen Display</td>
<td>Fixed-width font indicates CLI prompts, CLI commands entered by the user, and system messages displayed on the console.</td>
</tr>
<tr>
<td>all</td>
<td>When a parameter is required to define a range of ports or parameters and all is an option, the default for the command is <strong>all</strong> when no parameters are defined. For example, the command <code>interface range port-channel</code> has the option of either entering a range of channels, or selecting all. When the command is entered without a parameter, it automatically defaults to all.</td>
</tr>
<tr>
<td>text</td>
<td>When free text can be entered as a parameter for a command (for example in command: <code>snmp-server contact</code>) if the text consists of multiple words separated by blanks, the entire string must appear in double quotes. For example: <code>snmp-server contact &quot;QA on floor 8&quot;</code></td>
</tr>
</tbody>
</table>
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 Gigabitethernet 1`, `show`, `interfaces` and `status` are keywords, `Gigabitethernet` is an argument that specifies the interface type, and `1` specifies the port.

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

```
switchxxxxxx(config)# username admin password alansmith
```

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 or the character `?` is entered in place of a parameter, the matched keyword or parameters for this command are displayed.

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

- Terminal Command Buffer
- Command Completion
- Interface Naming Conventions
- Keyboard Shortcuts

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.
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 216. By configuring 0, the effect is the same as disabling the history buffer system. For more information on configuring the command history buffer, refer to the `history size` 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 attempts to identify and complete the command. If the characters already entered are not sufficient 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.

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

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device. 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, ensure that the following conditions exist:

- A device configuration mode has been accessed.
- The commands contain no encrypted data, like 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 (for instance in the `enable password` command).
Interface Naming Conventions

Interface ID

Within the CLI, interfaces are denoted by concatenating the following elements:

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

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

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<first-port-channel-number>
[ - <last-port-channel-number>] |
tunnel<first-tunnel-number>[ - <last-tunnel-number>] |
vlan<first-vlan-id>[ - <last-vlan-id>]
```

Up to five ranges can be included.

**NOTE**
Range lists can contain either ports and port-channels or VLANs. Combinations of port/port-channels and VLANs are not allowed.

When a range list is defined, a space after the first entry and before the comma (,) must be entered. The space after the command is optional.
A sample of this command is shown in the example below:

```
console#configure
console(config-if)#interface range gi1-5, vlan 1-2
```

### IPv6z Address Conventions

The following describes how to write an IPv6z address, which is a link-local IPv6 address.

The format is: `<ipv6-link-local-address>%<egress-interface>`

where:

**egress-interface (also known as zone)** = `vlan<vlan-id>` | `po<number>` | `tunnel<number>` | `port<number>` | 0

If the egress interface is not specified, the default interface is selected. Specifying egress interface = 0 is equal to not defining an egress interface.

The following combinations are possible:

- **ipv6_address%egress-interface** - Refers to the IPv6 address on the interface specified.
- **ipv6_address%0** - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.
- **ipv6_address** - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

### System Modes

The default mode is Switch (Layer 2) system mode. To change the system mode of the switch to Router (Layer 3), use the `set system` command.

This command performs a system reboot.

In Switch system mode, the switch forwards packets as a VLAN-aware bridge. In Router system mode, the switch performs both IPv4 routing and VLAN-aware bridging.

If Router system mode is selected, a single IP address is supported on the default VLAN. The user also must configure a default gateway.
If Router system mode is selected, the user can manage the device on any IP interface configured on the device, as long as a default route is configured. In Router system mode, the switch routes traffic between IP VLANs, and bridges traffic with VLANs.

When the switch operates in Router system mode, the following features are not supported:

- MAC-based VLANs
- VLAN Rate Limit
- DVA, Multicast TV VLAN
- Per flow policing
2.1 enable

The **enable** EXEC mode command enters the Privileged EXEC mode.

**Syntax**

```
enable [privilege-level]
```

**Parameters**

*privilege-level*—Specifies the privilege level at which to enter the system. (Range: 1, 7, 15)

**Default Configuration**

The default privilege level is 15.

**Command Mode**

EXEC mode

**Example**

The following example enters privilege level 7.

```
switchxxxxxx# enable 7
enter password:**********
switchxxxxxx#Accepted
```

The following example enters privilege level 15.

```
switchxxxxxx# enable
enter password:**********
switchxxxxxx#Accepted
```
2.2 disable
The disable Privileged EXEC mode command leaves the Privileged EXEC mode and returns to the User EXEC mode.

Syntax

disable [privilege-level]

Parameters

privilege-level—Reduces the privilege level to the specified privileged level. If privilege level is left blank, the level is reduce to 1.

Default Configuration
The default privilege level is 1.

Command Mode
Privileged EXEC mode

Example
The following example returns the user to user level 7.

switchxxxxxx# disable 7
switchxxxxxx#

2.3 login
The login EXEC mode command enables changing the user that is logged in.
When this command is logged in, the user is prompted for a username/password.

Syntax

login

Parameters

N/A
Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example enters Privileged EXEC mode and logs in with the required username ‘bob’.

```
switchxxxxxx# login
User Name: bob
Password: *****
switchxxxxxx#
```

2.4 configure
The `configure` Privileged EXEC mode command enters the Global Configuration mode.

Syntax
`configure [terminal]`

Parameters
- `terminal`—Enter the Global Configuration mode with or without the keyword `terminal`.

Command Mode
Privileged EXEC mode

Example
The following example enters Global Configuration mode.

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

The `exit` command exits any mode and brings the user to the next higher mode in the CLI mode hierarchy.

**Syntax**

`exit`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

All.

**Examples**

The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# exit
```

2.6 exit (EXEC)

The `exit` EXEC mode command closes an active terminal session by logging off the device.

**Syntax**

`exit`

**Parameters**

N/A
Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example closes an active terminal session.

```bash
switchxxxxxx# exit
```

### 2.7 end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

**Syntax**

```bash
end
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

All

**Example**

The following example ends the Global Configuration mode session and returns to the Privileged EXEC mode.

```bash
switchxxxxxx(config)# end
switchxxxxxx#
```
2.8 help

The `help` command displays a brief description of the Help system.

Syntax

```
help
```

Parameters

N/A

Default Configuration

N/A

Command Mode

All

Example

The following example describes the Help system.

```
switchxxxxxx# help
```

Help may be requested at any point in a command by entering a question mark `?`. If nothing matches the currently entered incomplete command, the help list is empty. This indicates that there is no command matching the input as it currently appears. If the request is within a command, press the Backspace key and erase the entered characters to a point where the request results in a match.

Help is provided when:

1. There is a valid command and a help request is made for entering a parameter or argument (e.g. 'show ?'). All possible parameters or arguments for the entered command are then displayed.

2. An abbreviated argument is entered and a help request is made for arguments matching the input (e.g. 'show pr?').
2.9 history

The history Line Configuration mode command enables saving commands that have been entered. Use the no form of this command to disable the command.

Syntax

history

no history

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Line Configuration mode

User Guidelines

This command enables saving user-entered commands for a specified line. You can return to previous lines by using the up or down arrows.

It is effective from the next time that the user logs in via console/telnet/ssh.

The following are related commands:

- Use the terminal history size EXEC mode command to enable or disable this command for the current terminal session.
- Use the history size Line Configuration mode command to set the size of the command history buffer.

Example

The following example enables the command for Telnet.

switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history
2.10 history size

The **history size** Line Configuration mode command changes the maximum number of user commands that are saved in the history buffer for a particular line. Use the **no** form of this command to reset the command history buffer size to the default value.

**Syntax**

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

**Parameters**

- **number-of-commands**—Specifies the number of commands the system records in its history buffer. (Range: 10–207)

**Default Configuration**

The default command history buffer size is 10 commands.

**Command Mode**

Line Configuration mode

**User Guidelines**

This command configures the command history buffer size for a particular line. It is effective from the next time that the user logs in via console/telnet/ssh.

Use the `terminal history size` EXEC mode command to configure the command history buffer size for the current terminal session.

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
switchxxxxxxx(config-line)# history size 100
```
2.11 terminal history

The terminal history EXEC mode command enables the command history function for the current terminal session, meaning it is not stored in the Running Configuration file. Use the no form of this command to disable the command.

Syntax

terminal history

terminal no history

Default Configuration

The default configuration for all terminal sessions is defined by the history Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the history Line Configuration mode command.

This command is effective immediately.

Example

The following example disables the command history function for the current terminal session.

switchxxxxxx# terminal no history

2.12 terminal history size

The terminal history size EXEC mode command changes the command history buffer size for the current terminal session, meaning it is not stored in the Running Configuration file. Use the no form of this command to reset the command history buffer size to the default value.

Syntax

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

Parameters

number-of-commands—Specifies the number of commands the system maintains in its history buffer. (Range: 10–207)

Default Configuration

The default configuration for all terminal sessions is defined by the history size Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The terminal history size EXEC command changes the command history buffer size for the current terminal session. Use the history Line Configuration mode command to change the default history buffer size.

The maximum number of commands in all buffers is 207.

Example

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
switchxxxxxx#terminal history size 20
```

2.13  terminal datadump

The terminal datadump EXEC mode command enables dumping all the output of a show command without prompting. Use the no form of this command to disable dumping.

Syntax

terminal datadump

terminal no datadump

Parameters

N/A
Default Configuration
When printing, dumping is disabled and printing is paused every 24 lines.

Command Mode
EXEC mode

User Guidelines
By default, a More prompt is displayed when the output contains more than 24 lines. Pressing the Enter key displays the next line; pressing the Spacebar displays the next screen of output.

The terminal datadump command enables dumping all output immediately after entering the show command by removing the pause.

The width is currently not limited (previously the limit was 77 chars), and the width of the line being printed on the terminal is based on the terminal itself.

This command is relevant only for the current session.

Example
The following example dumps all output immediately after entering a show command.

```
switchxxxxx# terminal datadump
```

2.14 terminal width
Use the terminal width EXEC mode command to determine the width of the display for the echo input to CLI sessions and configuration files. Use terminal no width to return to the default.

The command is per session and will not be saved in the configuration database.

Syntax
```
terminal width number-of-characters
terminal no width
```
Parameters

**number-of-characters** - Specifies the number of characters to be displayed for the echo output of the CLI commands and the configuration file, '0' means endless number of characters on a screen line. (Range: 0, 70-512)

Default Configuration

The default number of characters is 77.

Command Mode

Privileged EXEC mode

Example

The following example sets the terminal width to 100 characters

```plaintext
switchxxxxxx# terminal width 100
```

---

### 2.15 terminal prompt

Use the `terminal prompt` EXEC mode command to enable the terminal prompts. Use `terminal no prompt` command to disable the terminal prompts.

The command is per session and will not be saved in the configuration database.

Syntax

- `terminal prompt`
- `terminal no prompt`

Parameters

N/A

Default Configuration

The default configuration is prompts enabled.

Command Mode

Privileged EXEC mode
Example
The following example disables the terminal prompts

```
switchxxxxxx# terminal no prompt
```

2.16  **show history**

The **show history** EXEC mode command lists commands entered in the current session.

Syntax

```
show history
```

Parameters

N/A

Default Configuration

N/A

Command Mode

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 configuration modes.

Example

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
switchxxxxxx# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0
switchxxxxxx# show clock
```

15:29:03 Jun 17 2005
switchxxxxxx# show history
show version
show clock
show history
3 commands were logged (buffer size is 10)

2.17 show privilege

The `show privilege` EXEC mode command displays the current privilege level.

**Syntax**

```
show privilege
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays the privilege level for the user logged on.

```
switchxxxxxx# show privilege
Current privilege level is 15
```

2.18 do

The `do` command executes an EXEC-level command from Global Configuration mode or any configuration submode.
Syntax

do command

Parameters

command—Specifies the EXEC-level command to execute.

Command Mode

All configuration modes

Example

The following example executes the show vlan Privileged EXEC mode command from Global Configuration mode.

Example

switchxxxxxx(config)# do show vlan

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>gi1-39, Po1, Po2</td>
<td>other</td>
<td>Required</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>gi1</td>
<td>dynamicGvrp</td>
<td>Required</td>
</tr>
<tr>
<td>10</td>
<td>v0010</td>
<td>gi1</td>
<td>permanent</td>
<td>Not Required</td>
</tr>
<tr>
<td>11</td>
<td>V0011</td>
<td>gi1, gi3</td>
<td>permanent</td>
<td>Required</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>gi1</td>
<td>permanent</td>
<td>Required</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td>gi1, gi3</td>
<td>permanent</td>
<td>Required</td>
</tr>
<tr>
<td>31</td>
<td>31</td>
<td>gi1</td>
<td>permanent</td>
<td>Required</td>
</tr>
<tr>
<td>91</td>
<td>91</td>
<td>gi1, gi4</td>
<td>permanent</td>
<td>Required</td>
</tr>
<tr>
<td>4093</td>
<td>guest-vlan</td>
<td>gi1, gi3</td>
<td>permanent</td>
<td>Guest</td>
</tr>
</tbody>
</table>

switchxxxxxx(config)#

2.19  banner login

Use the banner login command in Global Configuration mode to specify a message to be displayed before the username and password login prompts. This banner is applied automatically on all the CLI interfaces: Console, Telnet and SSH
and also on the WEB GUI. Use the no form of this command to delete the existing login banner.

**Syntax**

```plaintext
banner login d message-text d
no banner login
```

**Parameters**

- **d**—Delimiting character of user’s choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
- **message-text**—Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of `$(token)` in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, you must press <Enter> to continue).

**Default Configuration**

Disabled (no Login banner is displayed).

**Command Mode**

Global Configuration mode

**User Guidelines**

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of `$(token)` in the message text to customize the banner. The tokens are described in the table below:

<table>
<thead>
<tr>
<th>Token</th>
<th>Information displayed in the banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(hostname)</td>
<td>Displays the host name for the device.</td>
</tr>
<tr>
<td>$(domain)</td>
<td>Displays the domain name for the device.</td>
</tr>
<tr>
<td>$(bold)</td>
<td>Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.</td>
</tr>
<tr>
<td>$(inverse)</td>
<td>Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.</td>
</tr>
</tbody>
</table>
Use the no banner login Line Configuration command to disable the Login banner on a particular line or lines.

Example
The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the $(token) syntax is replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain)
%
When the login banner is executed, the user will see the following banner:
You have entered host123.ourdomain.com
```

2.20 show banner
Use the show banner commands in EXEC mode to display the banners that have been defined.

Syntax
show banner login

Parameters
This command has no arguments or keywords.

Command Mode
EXEC mode

Examples

<table>
<thead>
<tr>
<th>Token</th>
<th>Information displayed in the banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(contact)</td>
<td>Displays the system contact string.</td>
</tr>
<tr>
<td>$(location)</td>
<td>Displays the system location string.</td>
</tr>
<tr>
<td>$(mac-address)</td>
<td>Displays the base MAC address of the device.</td>
</tr>
</tbody>
</table>
switchxxxxxx# show banner login

-----------------------------------------------
Banner: Login
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
3.1 macro name

Use the **macro name** Global Configuration mode command to define a macro. There are two types of macros that can be defined:

- Global macros define a group of CLI commands that can be run at any time.
- Smartport macros are associated with Smartport types (**Smartport Commands**). For each Smartport macro there must be an anti macro (a macro whose name is concatenated with `no_`). The anti macro reverses the action of the macro.

If a macro with this name already exists, it overrides the previously-defined one. Use the **no** form of this command to delete the macro definition.

**Syntax**

```text
macro name [macro-name]
no macro name [macro-name]
```

**Parameters**

- `macro-name`—Name of the macro. Macro names are case sensitive.

**Default Configuration**

N/A

**Command Mode**

Global Configuration mode

**User Guidelines**

A macro is a script that contains CLI commands and is assigned a name by the user. It can contain up to 3000 characters and 200 lines.

**Keywords**

Macros may contain keywords (parameters). The following describes keywords:
• A macro can contain up to three keywords.
• All matching occurrences of the keyword are replaced by the corresponding value specified in macro.
• Keyword matching is case-sensitive
• Applying a macro with keywords does not change the state of the original macro definition.

User Feedback
The behavior of a macro command requiring user feedback is the same as if the command is entered from terminal: it sends its prompt to the terminal and accepts the user reply.

Creating a Macro
Use the following guidelines to create a macro:

• Use macro name to create the macro with the specified name.
• Enter one macro command per line.
• Use the `@` character to end the macro.
• Use the `#` character at the beginning of a line to enter a comment in the macro.

In addition, `#` is used to identify certain preprocessor commands that can only be used within a macro. There are two possible preprocessor commands:

- `#macro key description` - Each macro can be configured with up to 3 keyword/description pairs. The keywords and descriptions are displayed in the GUI pages when the macro is displayed.

The syntax for this preprocessor command is as follows:

```
#macro key description $keyword1 description1 $keyword2 description2 $keyword3 description3
```

A keyword must be prefixed with `$`.

- `#macro keywords` - This instruction enables the device to display the keywords as part of the CLI help. It accepts up to 3 keywords. The command creates a CLI help string with the keywords for the macro. The help string will be displayed if help on the macro is requested from the macro and macro global commands. The GUI also uses the keywords specified in the command as the parameter names for the macro. See
Example 2 and 3 below for a description of how this command is used in the CLI.

The syntax for this preprocessor command is as follows:

```
#define keywords $keyword1 $keyword2 $keyword3
```

where $keywordn is the name of the keyword.

**Editing a Macro**

Macros cannot be edited. Modify a macro by creating a new macro with the same name as the existing macro. The newer macro overwrites the existing macro.

The exceptions to this are the built-in macros and corresponding anti-macros for the Smartport feature. You cannot override a Smartport macro. To change a Smartport macro, create a new macro (my_macro) and an anti macro (no_my_macro) and associate it with the Smartport type using `macro auto user smartport macro`.

**Scope of Macro**

It is important to consider the scope of any user-defined macro. Because of the potential hazards of applying unintended configurations, do not change configuration modes within the macro by using commands such as `exit`, `end`, or `interface interface-id`. With a few exceptions, there are other ways of executing macros in the various configuration modes. Macros may be executed in Privileged Exec mode, Global Configuration mode, and Interface Configuration mode (when the interface is NOT a VLAN.).

**Examples**

**Example 1** -The following example shows how to create a macro that configures the duplex mode of a port.

```
switchxxxx(config)# macro name dup
Enter macro commands one per line. End with the character '@'.
#define macro description dup
duplex full
negotiation
@
```

**Example 2** -The following example shows how to create a macro with the parameters: DUPLEX and SPEED. When the macro is run, the values of DUPLEX
and SPEED must be provided by the user. The #macro keywords command enables the user to receive help for the macro as shown in Example 3.

```
switchxxxxxx(config) # macro name duplex
Enter macro commands one per line. End with the character '@'.

duplex $DUPLEX
no negotiation
speed $SPEED

#macro keywords $DUPLEX $SPEED
@
```

**Example 3** - The following example shows how to display the keywords using the help character '?' (as defined by the #macro keywords command above) and then run the macro on the port. The #macro keywords command entered in the macro definition enables the user to receive help for the macro, as shown after the words e.g. below.

```
switchxxxxxx(config-if)#interface gi1
switchxxxxxx(config-if)#macro apply duplex ?
    WORD <1-32>  Keyword to replace with value e.g. $DUPLEX, $SPEED
    <cr>
switchxxxxxx(config-if)#macro apply duplex $DUPLEX ?
    WORD<1-32>  First parameter value
    <cr>
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED ?
    WORD<1-32>  Second parameter value

switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED 100
```

### 3.2 macro

Use the **macro apply**/trace Interface Configuration command to either:

- Apply a macro to an interface without displaying the actions being performed
- Apply a macro to the interface while displaying the actions being performed
Macro Commands

Syntax

macro {apply | trace} macro-name [parameter-name1 {value}] [parameter-name2 {value}] [parameter-name3 {value}]

Parameters

- **apply**—Apply a macro to the specific interface.
- **trace**—Apply and trace a macro to the specific interface.
- **macro-name**—Name of the macro.
- **parameter-name value**—(Optional) For each parameter defined in the macro, specify its name and value. You can enter up to three parameter-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the parameter name in the macro are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

The **macro apply** command hides the commands of the macro from the user while it is being run. The **macro trace** command displays the commands along with any errors which are generated by them as they are executed. This is used to debug the macro and find syntax or configuration errors.

When you run a macro, if a line in it fails because of a syntax or configuration error, the macro continues to apply the remaining commands to the interface.

If you apply a macro that contains parameters in its commands, the command fails if you do not provide the values for the parameters. You can use the **macro apply macro-name** with a '?' to display the help string for the macro keywords (if you have defined these with the **macro keywords** preprocessor command).

Parameter (keyword) matching is case sensitive. All matching occurrences of the parameter are replaced with the provided value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

When you apply a macro to an interface, the switch automatically generates a macro description command with the macro name. As a result, the macro name is
appended to the macro history of the interface. The `show parser macro` command displays the macro history of an interface.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When a macro is applied to an interface range, it is applied sequentially to each interface within the range. If a macro command fails on one interface, it is nonetheless attempted to be applied and may fail or succeed on the remaining interfaces.

**Examples**

**Example 1** - The following is an example of a macro being applied to an interface with the trace option.

```
switchxxxxxx(config) # interface gi1
switchxxxxxx(config-if) # macro trace dup $DUPLEX full $SPEED 100
  Applying command... 'duplex full'
  Applying command... 'speed 100'
switchxxxxxx(config-if) #
```

**Example 2** - The following is an example of a macro being applied without the trace option.

```
switchxxxxxx(config) # interface gi1
switchxxxxxx(config-if) # macro apply dup $DUPLEX full $SPEED 100
switchxxxxxx(config-if) #
```

**Example 3** - The following is an example of an incorrect macro being applied.

```
switchxxxxxx(config-if)#macro trace dup
Applying command...'duplex full'
Applying command...'speed auto'
% bad parameter value
```

**3.3 macro description**

Use the `macro description` Interface Configuration mode command to append a description, for example, a macro name, to the macro history of an interface. Use the `no` form of this command to clear the macro history of an interface. When the
Macro Commands

When a macro is applied to an interface, the switch automatically generates a macro description command with the macro name. As a result, the name of the macro is appended to the macro history of the interface.

Syntax

```
macro description text

no macro description
```

Parameters

text—Description text. The text can contain up to 160 characters. The text must be double quoted if it contains multiple words.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

When multiple macros are applied on a single interface, the description text is a concatenation of texts from a number of previously-applied macros.

To verify the settings created by this command, run `show parser macro`.

Example

```
switchxxxxxx(config)#interface gi2
switchxxxxxx(config-if)#macro apply dup
switchxxxxxx(config-if)#exit
switchxxxxxx(config)#interface gi3
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED 100
switchxxxxxx(config-if)#macro description dup
switchxxxxxx(config-if)#macro description duplex
switchxxxxxx(config-if)#end
switchxxxxxx#show parser macro
description:
```

Global Macro(s):
### Macro Commands

<table>
<thead>
<tr>
<th>Interface</th>
<th>Macro Description(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi2</td>
<td>dup</td>
</tr>
<tr>
<td>gi3</td>
<td>duplex</td>
</tr>
</tbody>
</table>

```
switchxxxxxx#configure
switchxxxxxx(config)#interface gi2
switchxxxxxx(config-if)#no macro description
switchxxxxxx(config-if)#end
switchxxxxxx#show parser macro description
```

**Global Macro(s):**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Macro Description(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi3</td>
<td>duplex</td>
</tr>
</tbody>
</table>

```
switchxxxxxx#
```

### 3.4 macro global

Use the `macro global` Global Configuration command to apply a macro to a switch (with or without the trace option).

**Syntax**

```
macro global [apply | trace] macro-name [parameter-name1 {value}] [parameter-name2 {value}] [parameter-name3 {value}]
```

**Parameters**

- **apply**—Apply a macro to the switch.
- **trace**—Apply and trace a macro to the switch.
- **macro-name**—Specify the name of the macro.
- **parameter-name value**—(Optional) Specify the parameter values required for the switch. You can enter up to three parameter-value pairs. Parameter
Keyword matching is case sensitive. All matching occurrences of the parameters are replaced with the corresponding value.

Default Configuration
The command has no default setting.

Command Mode
Global Configuration mode

User Guidelines
If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

If you apply a macro that contains keywords in its commands, the command fails if you do not specify the proper values for the keywords when you apply the macro. You can use this command with a '?' to display the help string for the macro keywords. You define the keywords in the help string using the preprocessor command `#macro keywords` when you define a macro.

When you apply a macro in Global Configuration mode, the switch automatically generates a global macro description command with the macro name. As a result, the macro name is appended to the global macro history. Use `show parser macro` to display the global macro history.

Example.

The following is an example of a macro being defined and then applied to the switch with the trace option.

```
switchxxxxxx(config)#  macro name console-timeout
Enter macro commands one per line. End with the character '@'.
line console
exec-timeout $timeout-interval
@
switchxxxxxx(config)#  macro global trace console-timeout $timeout-interval 100
```
Applying command… ‘line console’
Applying command… ‘exec-timeout 100’

switchxxxxxx(config)#

3.5 macro global description

Use the macro global description Global Configuration command to enter a
description which is used to indicate which macros have been applied to the
switch. Use the no form of this command to remove the description.

Syntax

macro global description text
no macro global description

Parameters

text—Description text. The text can contain up to 160 characters.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

When multiple global macros are applied to a switch, the global description text is
a concatenation of texts from a number of previously applied macros.

You can verify your settings by entering the show parser macro description
privileged EXEC mode command.

Examples

switchxxxxxx(config)# macro global description "set console timeout interval"
### 3.6 show parser macro

Use the `show parser macro` User EXEC mode command to display the parameters for all configured macros or for one macro on the switch.

**Syntax**

```
show parser macro [brief | description [interface interface-id | detailed] | name macro-name]
```

**Parameters**

- **brief**—Display the name of all macros.
- **description [interface interface-id]**—Display the macro descriptions for all interfaces or if an interface is specified, display the macro descriptions for that interface.
- **name macro-name**—Display information about a single macro identified by the macro name.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display description of all macros on present ports. If detailed is not used, only present ports are displayed.

**Command Mode**

User EXEC mode

**Examples**

**Example 1** - This is a partial output example from the `show parser macro` command.

```
switchxxxxxx# show parser macro
Total number of macros = 6
-----------------------------------------------
Macro name : cisco-global
Macro type : default global
```
# Enable dynamic port error recovery for link state failures

</output truncated>

Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

</output truncated>

**Example 2** - This is an example of output from the *show parser macro name* command.

```
switchxxxxxx# show parser macro standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

**Example 3** - This is an example of output from the *show parser macro brief* command.

```
switchxxxxxx# show parser macro brief
default global : cisco-global
default interface: cisco-desktop
```
default interface: cisco-phone
default interface: cisco-switch
default interface: cisco-router
customizable: snmp

This is an example of output from the `show parser macro description` command.
switchxxxxxx# show parser macro description
Global Macro(s): cisco-global

Example 4 - This is an example of output from the `show parser macro description interface` command.

switchxxxxxx# show parser macro description interface gi2
Interface Macro Description
---------------------------------------------------------------------
gi2 this is test macro
---------------------------------------------------------------------
RSA and Certificate Commands

Keys and Certificates

The device automatically generates default RSA/DSA keys and certificates at following times:

- When the device is booted following a software upgrade.
- When the device is booted with an empty configuration.
- When user-defined keys/certificates are deleted.

Some commands in this section are used to generate user-defined RSA/DSA keys and certificates that replace the default keys and are used by SSL and SSH server commands. Other commands can be used to import these keys from an external source.

These keys and certificates are stored in the configuration files.

Table 1 describes when these keys/certificates are displayed.

<table>
<thead>
<tr>
<th>File Type Being Displayed</th>
<th>What is Displayed in a Show Command Without Detailed</th>
<th>What is Displayed in a Show Command With Detailed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Config</td>
<td>Only user-defined keys/certificates.</td>
<td>Option is not supported.</td>
</tr>
<tr>
<td>Running Config</td>
<td>Keys are not displayed.</td>
<td>All keys (default and user-defined)</td>
</tr>
<tr>
<td>Text-based CLI (local backup config. file, mirror config. file or remote backup config. file)</td>
<td>Keys are displayed as they were copied. There is no distinction here between default and user-defined keys.</td>
<td>Option is not supported.</td>
</tr>
</tbody>
</table>
**Table 2** describes how keys/certificates can be copied from one type of configuration file to another (using the `copy` command).

**Table 2: Copying Keys/Certificates**

<table>
<thead>
<tr>
<th>Destination File Type</th>
<th>Copy from Running Config.</th>
<th>Copy from Startup Config.</th>
<th>Copy from Remote/Local Backup Config. File or Mirror Config. File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Config.</td>
<td>All keys/certificates are copied (but only user-defined ones can be displayed)</td>
<td>Option is not supported.</td>
<td>All keys/certificates present in this file are copied.²</td>
</tr>
<tr>
<td>Running Config</td>
<td>N/A</td>
<td>Only user defined.</td>
<td>All keys/certificates present in this file are copied.²</td>
</tr>
<tr>
<td>Text-based CLI (local backup config. file, mirror config. file or remote backup config. file)</td>
<td>All keys (default and user)</td>
<td>Only user defined.</td>
<td>All keys/certificates present in this file are copied.²</td>
</tr>
</tbody>
</table>

1. If the Running Configuration file on the device contains default keys (not user-defined ones), the same default keys remain after reboot.
2. In a text-based configuration file, there is no distinction between automatically-defined, default keys and user-defined keys.

### 4.1 crypto key generate dsa

The `crypto key generate dsa` Global Configuration mode command generates a public and private DSA key (DSA key pair).

**Syntax**

```
crypto key generate dsa
```

**Parameters**

N/A

**Default Configuration**

The application creates a default key automatically.

**Command Mode**

Global Configuration mode
User Guidelines

DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Erasing of the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example generates a DSA key pair.

```
switchxxxxxx(config)# crypto key generate dsa
```

The SSH service is generating a private DSA key.

This may take a few minutes, depending on the key size.

.........

4.2 crypto key generate rsa

The crypto key generate rsa Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Parameters

N/A

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode
User Guidelines

RSA keys are generated in pairs - one public RSA key and one private RSA key. If the device already has RSA keys, a warning 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 device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example generates RSA key pairs where a RSA key already exists.

```plaintext
switchxxxxx(config)# crypto key generate rsa
Replace Existing RSA Key [y/n]? N
switchxxxxx(config)#
```

4.3 crypto key import

The crypto key import Global Configuration mode command imports the DSA/RSA key pair.

Use the no form of the command to remove the user key and generate a new default in its place.

Syntax

crypto key import {dsa | rsa}
encrypted key import {dsa | rsa}
no crypto key {dsa | rsa}

Parameters

N/A

Default Configuration

DSA and RSA key pairs do not exist.
**Command Mode**

Global Configuration mode

**User Guidelines**

DSA/RSA keys are imported in pairs - one public DSA/RSA key and one private DSA/RSA key.

If the device already has DSA/RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is saved in the Running Configuration file.

When using the **encrypted** key-word, the private key is imported in its encrypted form.

**Example**

The following example imports RSA key pairs where a RSA key already exists.

**Example 1**

Import plaintext key

```
switchxxxxxxx(config)# crypto key import rsa
Replace Existing RSA Key [y/n]? Y
-----BEGIN RSA PRIVATE KEY-----
MIICWQIBAAKgQDM3fV+7nopIQ512SU8gkekCzwbw0MiQF2pnaRA+IoKcs/DReyT21NU
pod1Dm1tefzVMmVo8skggfcHVxz3oPsgV9WRs9sxPbh2m5aY9VUTSDLMcIP0MK6L
kopUPrOEcm6EuEmivsCMAC714GsiLY17AxUm5qTkzT3wIBIwKBgAu06XT3rzWM3EBvPO
7pQlmELNqKAL7jQemF2uU3FtSbd0RmLuDYTKtE364ypY1/OGvMwTby4Wei9apQkrwe71b5
08eYGr80rPWUNE/6FeMDqnJQeZ381WHSw5qwAut+wOJ9yHyAQ7G2pPAs61M2YVP19HMb
YwBm3H47zjffrAkEa8CYFRVhNLwp29wEXSGTJe4QIdk8w2SUBNTxxrsqrzylo89yuyV/K8
qvzPuo0rondoPEXd81BqDir+qLI6Nv9wJBAJpwlZmmNEa1aC+UE4/VXnWMnH0HILVod
hPgozTFJaddE/OsDgKthfNhLrFw8yt81VPvZdwjyftn3bmYRwKvKQHSMwLtE/UHx0+0A
h6bR3jSt2D1269cvOxhrbMR+63DqAFrMFMwuhyVp8IXDvDp3rMSNISW9sYPvno/llAn+7T
OCQb1dUuz9Un02L76+uvd3ujc3q80A7zl/t2zRdo1KN/tYV2qVqE4Zx8++/gWmgjDa/d
209bLCQvIpKd/Hg+qsCQ3KSMwNTQ1151sf/iAQkMrnMs8ha59wo+tMfdk3/kZkTdTQT
knkRQxydFB7pQOjzbqFY5ZL21/R5HR+2r38Tc=
------END RSA PRIVATE KEY------
```
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMzd9X7ueikDmXaz1TyCr6QLPBvDQyJAXamdqtED4igpyz8NF7JPbU1Smh2UO
YyW15/NUGaaJWjyySC9ledXHPEG+yEX12Gz2zEWF89uHablpj1VS1JUMu2winQwrouSL1Q+
s49KboS4TCaK+wIwALuXgayItiLsDFSbmpOTNPFAgEj
-----END RSA PUBLIC KEY-----

Example 2 - Import encrypted key
encrypted crypto key import rsa

---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
84et9C2XUfcRlpemuGINAyglwfkKjCDM6m2OrsALHScqLh0wMSSYNIT1IFZP1kEVHH
FptlaECzi7HfGlcplPMZjnl+HaXBTqjPD4tEtbpScXqrg6ml/0/EnwPFK2TrmUy01Ifw18
E/mMFX3i/2rRzLkBEeasjtrA6Q62g15naRw12zKoges+GNeibtv2YSk1jzr56Lur6f7Xu5i
KMcU2b2NsuSD5yW8R/xOCW2elqDDz/biA2gSgd6Fvn2Hv48bTC55eCRxRsD2MmbExtudz
+RQRzjcGMByP6HzkD66z8HmSh0U+Rh7DMLK9U4Sr+Pr1vyWUJ1Ekogz906a2oIgP4tg4m
VDy/K/G/sI5nVL0+br8LFUXO/U5shoBcyRUFO2fHYKrzlt1pT5Rw+Pht6/+EXKG9E+TRs
1UADMltCrvs+lsB331BdvoRDd198YaA2ht2ay1TkbMqCubdf10+74UOqa/b+bp67wCYKe9
yen418MaYkthcJHBQmp7szUSQZGP34VPmOMyZzon68S/zo77cy9ihRZx9c1lLyYhnDiXYP
dgXYHw6kCTcTj6LrUSUQxCj93su892IWNn50wdgQnLSpvfnabv2GMyhmmavL7JJ7/UCfO
61q5D4Pj67V2xL7PqyHNX931rseTzPujlp1kSLCFZ5uqTMbWwYQEXKHD10x35vlGou5tky
9LgiwG4d+9edctZzageq5cgjnsZWjgqU0b4m4hIreyOdHdiUPPRxkoYhGOGnJuvxC9T9
K6BF1wBTdDQS+Gu47/0/g0/Rd0/5qqsGkzqHsRJ53WTOQ1bhHMtMLPpw2nXzvfGwWL/bu
Qh2ZSzRonG6MX1cPf7KT7T4Fq2w2k3TgtNBvVH8x60nCaThmg1N2s50gRyXd9Tf++6nY
RfMNNCSV+9jQKQP7zaGc8jU+d72jvSwppSr032Hy+Ipx2ujk+/X5oawZL5NkaeEQTQRX
RSL55S05NP0js/pC9h7GvJYo2m7HQDpSUEfTID1VoCwC2skdA96aF/Axj2XlweQd5
lk7m0/mMNaJrSNk6y33LlcRjIxpNNJ9k9kRPFKGMFObrfENKteDftjQ==
---- END SSH2 PRIVATE KEY ----

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABAIwAAAIEAvRhsKry6NMKymb+yWEp9042vupLvYVq3ngt1sB9JH
4.4 show crypto key

The show crypto key Privileged EXEC mode command displays the device’s SSH private and public keys for both default and user-defined keys.

Syntax

show crypto key [mypubkey] [rsa | dsa]

Parameters

- mypubkey—Displays only the public key.
- rsa—Displays the RSA key.
- dsa—Displays the DSA key.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

See Keys and Certificates for information on how to display and copy these keys.

Example

The following example displays the SSH public DSA keys on the device.

```
switchxxxxxx# show crypto key mypubkey dsa

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzN31fu56KSEOZdrGVPIJHpAs8G8NDIkB
dqZ2q0QPiKcnLpw0Xsk9tTVKaHzQ5jJbXn81QZpolaPLJIIH3B1cc96D7IFf
```
4.5 `crypto certificate generate`

The `crypto certificate generate` Global Configuration mode command generates a self-signed certificate for HTTPS.

**Syntax**

```plaintext
crypto certificate number generate [key-generate [length]] [cn common-name] [ou organization-unit] [or organization] [loc location] [st state] [cu country] [duration days]
```

**Parameters**

- **number**—Specifies the certificate number. (Range: 1–2)

- **key-generate length**—Regenerates SSL RSA key and specifies the SSL's RSA key length. (Range: 512–2048)

  The following elements can be associated with the key. When the key is displayed, they are also displayed.

  - **cn common-name**—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).

  - **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)

  - **or organization**—Specifies the organization name. (Length: 1–64 characters)

  - **loc location**—Specifies the location or city name. (Length: 1–64 characters)

  - **st state**—Specifies the state or province name. (Length: 1–64 characters)

  - **cu country**—Specifies the country name. (Length: 2 characters)
- **duration days**—Specifies the number of days a certification is valid. (Range: 30–3650)

**Default Configuration**

The default SSL’s RSA key length is 1024.

If `cn common-name` is not specified, it defaults to the device’s lowest static IPv6 address (when the certificate is generated), or to the device’s lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If `duration days` is not specified, it defaults to 365 days.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the RSA key does not exist, you must use the parameter `key-generate`.

If both certificates 1 and 2 have been generated, use `ip https certificate` to activate one of them.

See [Keys and Certificates](#) for information on how to display and copy these certificates.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

**Example**

The following example generates a self-signed certificate for HTTPS whose length is 2048 bytes.

```bash
switchxxxxxx(config)# crypto certificate 1 generate key-generate 2048
```

### 4.6 crypto certificate request

The `crypto certificate request` Privileged EXEC mode command generates and displays a certificate request for HTTPS.
Syntax

```
crypto certificate number request [cn common-name] [ou organization-unit] [or organization] [loc location] [st state] [cu country]
```

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
  - **cn common-name**—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
  - **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)
  - **or organization**—Specifies the organization name. (Length: 1–64 characters)
  - **loc location**—Specifies the location or city name. (Length: 1–64 characters)
  - **st state**—Specifies the state or province name. (Length: 1–64 characters)
  - **cu country**—Specifies the country name. (Length: 2 characters)

Default Configuration

If **cn common-name** is not specified, it defaults to the device’s lowest static IPv6 address (when the certificate is generated), or to the device’s lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command to generate the keys. The certificate fields must be re-entered.
After receiving the certificate from the Certification Authority, use the `crypto certificate import` Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

See **Keys and Certificates** for information on how to display and copy these certificates.

**Example**

The following example displays the certificate request for HTTPS.

```plaintext
switchxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAXczAJBgNVBAgTBkN0c2VydGlmaWVyMQswCQYDVQQGEwRUSUNB
EyMwY DAYDVQU实践中CN=example.com
.......

4.7 crypto certificate import

The `crypto certificate import` Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the RSA key-pair can also be imported.

Use the no form of the command to delete the user-defined keys and certificate.

**Syntax**

- `crypto certificate number import`
- `encrypted crypto certificate number import`
- `no crypto certificate number`
Parameters

number—Specifies the certificate number. (Range: 1–2)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

To end the session (return to the command line to enter the next command), enter a blank line.

The imported certificate must be based on a certificate request created by the crypto certificate request privileged EXEC command.

If only the certificate is imported, and the public key found in the certificate does not match the device's SSL RSA key, the command fails. If both the public key and the certificate are imported, and the public key found in the certificate does not match the imported RSA key, the command fails.

This command is saved in the Running configuration file.

When using the encrypted form of the command, only the private key must be in encrypted format.

See Keys and Certificates for information on how to display and copy these certificates.

Examples

Example 1 - The following example imports a certificate signed by the Certification Authority for HTTPS.

switchxxxxxx(config)# crypto certificate 1 import

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGALUEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMIIBIQMBAGC
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
Example 2: The following example imports a certificate signed by the Certification Authority for HTTPS, and the RSA key-pair.

```bash
switchxxxxxx(config)# crypto certificate 1 import
```

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

```
-----BEGIN RSA PRIVATE KEY-----
ACnrqImEgl1XkwBuZU1a09h9q9IGlQsknKf7/7au4GPvqyt5vdf77uQ5CPf49JWQu07cVxh
20wrBhjg869vLU1uM9p1IXPmk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevK6H
TGB7vMxi+hV1bL9zygvmQ6/+6Qfqa51c4nP/8a6NjO/2OAgvNAMKn2Wau+tGUoAgL0b/C
11EqgCq5mT7+V0FhPS04dUu+NwLl1Ycb1Fb7MFOaA0N+y+2WocGp0pxOVDa9ENy17qszZ
MWmCfXu52/IxC7f8FWnEBtk+4V81Xqa7K6ET657xS7m8yTJFL2JyVawGKnIUs6uTzhhw
09WWe8wsvn/7wbpri1yOwMh2GZI3Yq6aML648+j5M9b1Jr2W32Q4dQ4Gt5bc4PR4s3A3CRBx
WuGoazpXH20s4+7awmNztS0xI4ek43dRaodGKljoPqLHuXHUon7ZxL15UtP3sbH1+XI
B3u4EeeEngYmew5ob1lnvFSot+d5JHuRwEaRAIKfha34alVJaN+2AMCbohnpI31kreYo
A8L6LXWOpQ10amhNyf+RypFwHqOQs01PpIPKOHBT6npj39XmvyrRXvSnp5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSlhjApf51lQR1lJjb/mVt8+zpqccU94WQqsMrNFOFr5cbHu5V4
-----END RSA PRIVATE KEY-----
```

Certificate imported successfully.

- Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU=
- Valid From: Jan 24 18:41:24 2011 GMT
- Valid to: Jan 24 18:41:24 2012 GMT
- Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
- SHA1 Fingerprint: DC789788 DC88A988 127897BC BB789788
Example 3 - Import certificate with encrypted key

```
encrypted crypto certificate 1 import

-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMBIDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEgMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMzrYOOg9XMIAx0iqLlQJHd4xP+BHGZWwfkJkJUDBP2n52LxdDu1Rpb/h0+TZP0Fv387mIDqtnoF1NLwXkVKRM5LPka0L/halpYxp7EWAAt5iDBzSw5s04lv0bSN7oaGjFA6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hIxFDxeI8od3Yt3Dmf7KE/AmUV0If2yUu/RuxRwKhDp/1GrkI2tzLQz+a50x7K1ft/IcjzbBYXLvh45ASWG3TRv2WVKyWw89rPPXu5hXggEeTvWqpuS+gXrIqjWVWZd0n1XhMacofllgnEmweIzmrgXBe=
-----END CERTIFICATE-----
```

Certificate imported successfully.

Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
CNI2n5zf9oisMHOU6gsID4ysWVD1zNg0VQwD7RqKpL9wo3+YVFSVs6XCB7pDb71pPeF6a6
GD/crN28vTLGf/NpyKoCdAMRuqEQoapMo0Py2Cvy+sqLiv4ZKck1FPsLsVF7V7x7sh+zVa3
We84pmzyjGlY98t0tD3BSGHJ2xDCnTqTvUpffFEJJYrDGKCybqD0o3tD/ioUQ3UJgxDbGyw
aLlOavSjMyIWkdPjfcbn5MVrDU51aPcQJXwV3MYC8GQ4Hla6UDN6acUBa1UHqkJt+REWwO
DXpJmvmX4T/u5W4DPvELqTHyETxgQKNe1079gRi2yyLcybUokh+SP+XuRkG4IKknn8KyHtz
XeoDojSe6OYOQww2R0nAqn2ZPgrDzj0zTDL8qyvkurfW4jWa4c1sclhDEFtHH7NdDLjQ
FkPFNAkFMCymidapG+RwCvm31KBLcEpNXpEFe3v1mCeyN1pPe6sQmcBxa2VmbInutuP
CZM927oxkb41g+U50yQxGmK70Ez7mfs1FlDcmfqv0DH2N41t4KgqcsSjWPDQeYSZB+4FW
Qmy4ftF4wQdVCLy+WlVEp1jWpbrdCNxIS13RwucNeKrm9uf5Zuhd1FA9w8xSrJwuaq8q
zZFMmDMHPTey9AL02a1wpwHPbJKiCmddjHT94ugF30euyeni9sGN6Y063IvuKBY0nbwSAm
J0xsrvtq36cbkJYoZqME5LaxLNVQI4HBhPtUz+LNgYWb35S188kRejQM9eCyJsvLF
+yA15zAB2dTPqz017FNzhIrYvCqcCCXc+JbgP1pWYTDy0+m2H5v8Yv6s3y7f7Ec9+5/Sn
Vf8jpTLMWfGvF9U1Qw9bA8HA7K42E3RfZ1do0eUlXQKuRxLAKhf7D2hrE7udOmTF9
W3PqtJzbtjvMjM5/C+h0c60lNMp6qO7En78EdfaHpM4utMF01eKuzizenZQ==
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzeWjdz55F0wWv8a54k5VpuRtvle51zp7kzIL6mvCCX6J9c
kkr+TMe63b9t5RgwGPGwDHW3q5QkaqInzZ1hj2+A++mwCSuHilBhpFNFy/gmENIGq9f
puukcnoTvBNvz73V0xvw6w1UHMT0e0+QSbe7WwVAgMBAAE=

-----END RSA PUBLIC KEY-----

-----BEGIN CERTIFICATE-----
MIICHCCAYUCEFCCcI4/dhLSUhTwx0wbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAKG
A1UEBhMCICCAx7CjAIgBnvBAgTASAx7CjAIgNVBAcTASAx7EDA0BgNVBAgTBM2Zx4w
LjAxCAIgBnvBAoTASAx7CjAIgNVBAaTASAxHhcNMTIwNTixMTI1NzE2WchNMTMw
NTixMTI1NzE2WjBPMwQwCQYDVQQGEwIgIDEKMAgGA1UECBMBDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMMHC4wJluAaUDEKMAgGA1UECgMBDEKMAgGA1UEcMBDCbnAN
BgkqhkiG9w0BAQEFAAOCbQAwgYkCqYEyg3or5v2FOCvMR5a3PtKbBxyznItI
Wm5G2/V7mvX0nuTMgvqa81Jeq0nlySs5Mx9frdv231GDAY+2B4MfDrElCRoioF
FWHuPaB476abKweS61UGGkU0Vj+yCQ21ar1+m66Ryeh08E2/PvPdU7g/qHDVQcmX5
475Bjt7tbBUCAwEAATANBgkqhkiG9w0BAQEFAAOBjqAgwCQYDVQQGEwJ江北
2rd7c+czQ0e1e4CpEvV10CQQvgPa72pz+m/zvoFmAC5WjQngQMMwW8rNdvrsaSyE

-----END CERTIFICATE-----
Certificate imported successfully.

Issued by: C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788

4.8 show crypto certificate

The show crypto certificate Privileged EXEC mode command displays the device
SSL certificates and key-pair for both default and user defined keys.

Syntax

show crypto certificate [mycertificate] [number]

Parameters

- number—Specifies the certificate number. (Range: 1,3)
- mycertificate—Specifies that only the certificate will be displayed

Default Configuration

Certificate number 1.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example displays SSL certificate # 1 present on the
device.

switchxxxxxx# show crypto certificate mycertificate
Certificate 1:
Certificate Source: Default

------BEGIN CERTIFICATE------
dHmUGm9vdCBDZXJ0aWZpZXIxWDANBgkqhkiG9w0BAGQFAANLADBIAkEA4p4HS
nnH/xQSGA2f5kRBwU2X1xb7n8VFspTm1xyJlt11a1GaqchfMqqe0kmfhcoHSWr
yfIPD0NMWOTgDAwIDAQABo4IBojCCA24wEwYJKwYBBAGCNxQCBAYeBABAEEw
CwR0FBAQIdAgFGMA8GAL1dewEB/wQFMANMBAf8wHqYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBTLCCASkwgdKgnc+ggcyGc1sZGFwOi8v
L0VByb3h5JTIwU29mdHdcmUlMjBSb290JTIwQ2VydGlmaWVyLENOFXN1cnZl
------END CERTIFICATE------
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Fingerprint: DC789788 DC88A988 127897BC BB789788

Certificate 2:
Certificate Source: User-Defined

------BEGIN CERTIFICATE------
dHmUGm9vdCBDZXJ0aWZpZXIxWDANBgkqhkiG9w0BAGQFAANLADBIAkEA4p4HS
nnH/xQSGA2f5kRBwU2X1xb7n8VFspTm1xyJlt11a1GaqchfMqqe0kmfhcoHSWr
yfIPD0NMWOTgDAwIDAQABo4IBojCCA24wEwYJKwYBBAGCNxQCBAYeBABAEEw
CwR0FBAQIdAgFGMA8GAL1dewEB/wQFMANMBAf8wHqYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBTLCCASkwgdKgnc+ggcyGc1sZGFwOi8v
L0VByb3h5JTIwU29mdHdcmUlMjBSb290JTIwQ2VydGlmaWVyLENOFXN1cnZl
------END CERTIFICATE------
Issued by: www.verisign.com
Valid from: 8/9/2004 to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Fingerprint: DC789788 DC88A988 127897BC BB789788

Example 2:
The following example displays SSL certificate #1 present on the device and the key-pair.

```
switchxxxxxx# show crypto certificate 1
Certificate 1:
Certificate Source: Default
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIxNDABgkqhkiG9w0BAQEFAAQLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2Xixbn78VPSm1xyJlt11a1GqchfMqge0kmpfhoHSWr
yf1FpD0MWOTgDAIDAQABo4IBojC2CAZ4ewYJKwYBBAGCNxQCBAYeBEABADEmw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQQFMAHwAf8wHQYDVR0OBBYEFAs4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVROfBIIBLTCCASKwgdKggc+ggcyGcclsZGFwOi8v
L0VByb3h5JTIwU29mdHhcmlU0MjBSb290JTIwQ2VydgGlmaWVyLENOPXN1cnZl
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
ACnrqImEGLxkwBuZU1AO9nHaq9IGjnskf7/MauGPvqt5vfDF77uQ5CPF49JWQhu07cVXh
2wBrHJgB69vULujM9p1XFPmK8q3N7Jz1InYAYjHkkbE2BMskSA67t/UzVxeWKK6H
TGB7vWxi+hvbL9yvqmQ6/+6QfA5clc4nP/8a6qJO/O2AgvNAMNrz2Wa+tGUoAgL0b/C
11EoqzEq5mT7+VOFPb504dUU+NwLv1Ycb1Fb7MFoaA0N+y2NwGC0pxOVdA9ENY17qS
MwmCfXu52/IXC7fD8FWwzEbtks4V8IXqa7K6ET657xS7m87TUJFL2JyVawGKnUIs6TUzhW
dKWc0/e/vwMgPtLlWyXwnnaP0fAJ+PawOAdk75b079NBim3HcVXhWNzqfg2s3AYCRBx
WuGaozpHZ0s+7swnNzttS0xI4ek43d7RaoedgKljhPqLHzuXHuon7Zx15CUp3sh1H+XI
B3u4EEnGm5ewy5obv1nVFSot+d5JhRwzEaRAIKfcbHa34a1VJaN+2AMCB0hpI3IkreYo
A8Lk6UM0uIQAmhhYf+RPXPFQOs0lP1PHKBGTi6pj39XmviyRXvSpn5+eIYPheve5jYaEn
UeOnVZRhNCvnuJAYXLhjAprf5iIQrljiyb/mVt8+zpqcU9HCWqMsMrNPOFrSpcbHu5V4
ZX4jmd9Tj2mhekoQf1dwU2bfYkRYsK70ps8u7BtgpRFSRUr7g0LfzhzMuswoDSnB6SpkC
q17yZnBeRS0zrUDgHLLRfzwjmxOmxObyYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVufGfJYLLbUzmb6m6Ol3eWHeYd1ZMY4A3KLF2SXUd1ITXq8aME8DItSFB2
Cqy4Q5hInhgAmobkC96VRsUe2rzoNG4Qdkj2L9ukQ0oFBYNmbzHC7a+7043wFVmh+QOXf
TbnRDhIMVrZJGbzl1c91zGkyl121Xmyc0/rwsXDAeBj
```
-----END RSA PUBLIC KEY-----
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB78978
System Management Commands

5.1 ping

Use the ping EXEC mode command to send ICMP echo request packets to another node on the network.

Syntax

ping [ip] [ipv4-address | hostname] [size packet_size] [count packet_count] [timeout time_out]

ping ipv6 [ipv6-address | hostname] [size packet_size] [count packet_count] [timeout time_out]

Parameters

- ip—Use IPv4 to check the network connectivity.
- ipv6—Use IPv6 to check the network connectivity.
- ipv4-address—IPv4 address to ping.
- ipv6-address—Unicast or Multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. See IPv6z Address Conventions.
- hostname—Hostname to ping (Length: 1-160 characters. Maximum label size for each part of the host name: 63.)
- size packet_size—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64–1518, IPv6: 68–1518)
- count packet_count—Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- time timeout—Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).

Default Usage

N/A
Command Mode

EXEC mode

User Guidelines

Press Esc to stop pinging. Following are sample results of the ping command:

- Destination does not respond—If the host does not respond, a “no answer from host” appears within 10 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable—The switch found no corresponding entry in the route table.

See IPv6z Address Conventions.

When using the ping ipv6 command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the IPv6Z format. If the egress interface is not specified, the default interface is selected.

When using the ping ipv6 command with a Multicast address, the information displayed is taken from all received echo responses.

Examples

Example 1 - Ping an IP address.

```sh
switchxxxxxx# ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
---10.1.1.1 PING Statistics---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```
Example 2 - Ping 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 - Ping 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
```

```
switchxxxxxx# ping ipv6 FF02:1
Pinging FF02:1 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::33: icmp_seq=1. time=70 ms
64 bytes from 3003::11: icmp_seq=2. time=0 ms
64 bytes from 3003::55: icmp_seq=1. time=1050 ms
64 bytes from 3003::33: icmp_seq=2. time=70 ms
64 bytes from 3003::55: icmp_seq=2. time=1050 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
```
5.2 traceroute

To display the routes that packets will take when traveling to their destination, use the traceroute EXEC mode command.

Syntax

```
traceroute ip {ipv4-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
traceroute ipv6 {ipv6-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
```

Parameters

- `ip`—Use IPv4 to discover the route.
- `ipv6`—Use IPv6 to discover the route.
- `ipv4-address`—IPv4 address of the destination host.
- `ipv6-address`—IPv6 address of the destination host.
- `hostname`—Hostname of the destination host. (Length: 1-160 characters. Maximum label size for each part of the host name: 63.)
- `size packet_size`—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4: 64-1518, IPv6: 68-1518)
- `ttl max-ttl`—The largest TTL value that can be used. The default is 30. The traceroute command terminates when the destination is reached or when this value is reached. (Range: 1–255)
- `count packet_count`—The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)
timeout time_out—The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)

source ip-address—One of the interface addresses of the device to use as a source address for the probes. The device selects the optimal source address by default. (Range: Valid IP address)

tos tos—The Type-Of-Service byte in the IP Header of the packet. (Range: 0–255)

Default Usage
N/A

Command Mode
EXEC mode

User Guidelines
The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute command is not relevant to IPv6 link local addresses.

Example

switchxxxxxx# traceroute ip umaxpl.physics.lsa.umich.edu
Type Esc to abort.

Tracing the route to umaxpl.physics.lsa.umich.edu (141.211.101.64)

1 i2-gateway.stanford.edu (192.68.191.83) 0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162) 1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 33 msec 35 msec 35 msec
6 iplsgng-kscyng.abilene.ucaid.edu (198.32.8.80) 47 msec 45 msec 45 msec
7 so-0-2-0x1.aal.mich.net (192.122.183.9) 56 msec 53 msec 54 msec
8 atml-0x24.michnet8.mich.net (198.108.23.82) 56 msec 56 msec 57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu(141.211.5.22)58 msec 58msec 58 msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64) 62 msec 63 msec 63 msec
Trace completed

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates the sequence number of the router in the path to the host.</td>
</tr>
<tr>
<td>i2-gateway.stanford.edu</td>
<td>Host name of this router.</td>
</tr>
<tr>
<td>192.68.191.83</td>
<td>IP address of this router.</td>
</tr>
<tr>
<td>1 msec 1 msec 1 msec</td>
<td>Round-trip time for each of the probes that are sent.</td>
</tr>
</tbody>
</table>

The following are characters that can appear in the traceroute command output:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.</td>
</tr>
<tr>
<td>F</td>
<td>Fragmentation required and DF is set.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>R</td>
<td>Fragment reassembly time exceeded.</td>
</tr>
</tbody>
</table>
5.3 telnet

The `telnet` EXEC mode command logs on to a host that supports Telnet.

**Syntax**

```
telnet {ip-address | hostname} [port] [keyword...]
```

**Parameters**

- `ip-address`—Specifies the destination host IP address (IPv4 or IPv6).
- `hostname`—Specifies the destination host name. (Length: 1-160 characters. Maximum label size for each part of the host name: 63.)
- `port`—Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- `keyword`—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

**Default Configuration**

The default port is the Telnet port (23) on the host.

**Command Mode**

EXEC mode

**User Guidelines**

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Source route failed.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>
Special Telnet Sequences

<table>
<thead>
<tr>
<th>Telnet Sequence</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-shift-6-b</td>
<td>Break</td>
</tr>
<tr>
<td>Ctrl-shift-6-c</td>
<td>Interrupt Process (IP)</td>
</tr>
<tr>
<td>Ctrl-shift-6-h</td>
<td>Erase Character (EC)</td>
</tr>
<tr>
<td>Ctrl-shift-6-o</td>
<td>Abort Output (AO)</td>
</tr>
<tr>
<td>Ctrl-shift-6-t</td>
<td>Are You There? (AYT)</td>
</tr>
<tr>
<td>Ctrl-shift-6-u</td>
<td>Erase Line (EL)</td>
</tr>
</tbody>
</table>

At any time during an active Telnet session, available Telnet commands can be listed by pressing the `/help` keys at the system prompt.

A sample of this list follows.

```
switchxxxxxx# /help
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
/help suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened, enabling switching between the sessions. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the telnet EXEC mode command.

This command lists concurrent Telnet connections to remote hosts that were opened by the current Telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.
### Keywords Table

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/echo</td>
<td>Enables local echo.</td>
</tr>
<tr>
<td>/quiet</td>
<td>Prevents onscreen display of all messages from the software.</td>
</tr>
<tr>
<td>/source-interface</td>
<td>Specifies the source interface.</td>
</tr>
<tr>
<td>/stream</td>
<td>Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.</td>
</tr>
<tr>
<td>Ctrl-shift-6 x</td>
<td>Returns to the System Command Prompt.</td>
</tr>
</tbody>
</table>

### Ports Table

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>179</td>
</tr>
<tr>
<td>chargen</td>
<td>Character generator</td>
<td>19</td>
</tr>
<tr>
<td>cmd</td>
<td>Remote commands</td>
<td>514</td>
</tr>
<tr>
<td>daytime</td>
<td>Daytime</td>
<td>13</td>
</tr>
<tr>
<td>discard</td>
<td>Discard</td>
<td>9</td>
</tr>
<tr>
<td>domain</td>
<td>Domain Name Service</td>
<td>53</td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
<td>7</td>
</tr>
<tr>
<td>exec</td>
<td>Exec</td>
<td>512</td>
</tr>
<tr>
<td>finger</td>
<td>Finger</td>
<td>79</td>
</tr>
<tr>
<td>ftp</td>
<td>File Transfer Protocol</td>
<td>21</td>
</tr>
<tr>
<td>ftp-data</td>
<td>FTP data connections</td>
<td>20</td>
</tr>
<tr>
<td>gopher</td>
<td>Gopher</td>
<td>70</td>
</tr>
<tr>
<td>hostname</td>
<td>NIC hostname server</td>
<td>101</td>
</tr>
<tr>
<td>ident</td>
<td>Ident Protocol</td>
<td>113</td>
</tr>
<tr>
<td>irc</td>
<td>Internet Relay Chat</td>
<td>194</td>
</tr>
<tr>
<td>klogin</td>
<td>Kerberos login</td>
<td>543</td>
</tr>
<tr>
<td>kshell</td>
<td>Kerberos shell</td>
<td>544</td>
</tr>
<tr>
<td>login</td>
<td>Login</td>
<td>513</td>
</tr>
<tr>
<td>lpd</td>
<td>Printer service</td>
<td>515</td>
</tr>
<tr>
<td>nntp</td>
<td>Network News Transport Protocol</td>
<td>119</td>
</tr>
<tr>
<td>pim-auto-rp</td>
<td>PIM Auto-RP</td>
<td>496</td>
</tr>
</tbody>
</table>
Example

The following example displays logging in to IP address 176.213.10.50 via Telnet.

```
switchxxxxxx# telnet 176.213.10.50
```

### 5.4 resume

The **resume** EXEC mode command enables switching to another open Telnet session.

**Syntax**

```
resume [connection]
```

**Parameters**

- **connection**—Specifies the connection number. (Range: 1-4 connections.)

**Default Configuration**

The default connection number is that of the most recent connection.

**Command Mode**

EXEC mode
Example

The following command switches to open Telnet session number 1.

```
switchxxxxxx# resume 1
```

5.5 hostname

The `hostname` Global Configuration mode command specifies or modifies the device host name. Use the `no` form of the command to remove the existing host name.

Syntax

```
hostname name
no hostname
```

Parameters

- **Name**—Specifies the device host name. (Length: 1-160 characters. Maximum label size for each part of the host name: 63). The hostname must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens.

Default Configuration

No host name is defined.

Command Mode

Global Configuration mode

Example

The following example specifies the device host name as ‘enterprise’.

```
switchxxxxxx(config)# hostname enterprise
enterprise(config)#
```
5.6  reload

The `reload` Privileged EXEC mode command reloads the operating system at a user-specified time.

**Syntax**

```plaintext
reload [[in [hh:mm | mmm] | at hh:mm [day month]] | cancel]
```

**Parameters**

- **in hh:mm | mmm**—Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.

- **at hh:mm**—Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

- **day**—Number of the day in the range from 1 to 31.

- **month**—Month of the year.

- **cancel**—Cancels a scheduled reload.

**Default Usage**

N/A

**Command Mode**

Privileged EXEC mode

**User Guidelines**

The `at` keyword can be used only if the system clock has been set on the device. To schedule reloads across several devices to occur simultaneously, synchronize the time on each device with SNTP.

When you specify the reload time using the `at` keyword, if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the
current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

To display information about a scheduled reload, use the show reload command.

**Examples**

**Example 1**—The following example reloads the operating system.

```
switchxxxxxx# reload
This command will reset the whole system and disconnect your current session.
Do you want to continue? (y/n) [Y]
```

**Example 2**—The following example reloads the operating system in 10 minutes.

```
switchxxxxxx# reload in 10
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you want to continue? (y/n) [Y]
```

**Example 3**—The following example reloads the operating system at 13:00.

```
switchxxxxxx# reload at 13:00
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes). Do you want to continue? (y/n) [Y]
```

**Example 4**—The following example shows various usages of this command. Note that reload in 10 can work without the system clock being set, but reload at 17:12 Jun 6 requires that the system clock be set.

```
switchxxxxxx# show clock
*16:12:16 UTC Jun 4 2012//please note the '*' on the left side of the time
No time source
switchxxxxxx#reload in 10
```
This command will reset the whole system and disconnect your current session. Reload is scheduled to occur in 10 minutes. Do you want to continue? (Y/N)[N] Y

switchxxxxxx#reload at 17:12 Jun 6

Schedule-Reload is already set to occur in 9 minutes. Do you wish to override? (Y/N)[N] Y

To use the 'reload at' command please set the system clock time first.

switchxxxxxx#clock set 16:37:00 Jun 6 2012

switchxxxxxx#reload at 17:12 Jun 6

Schedule-Reload is already set for 16:45:17 UTC Wed Jun 6 2012 (in 8 minutes). Do you wish to override? (Y/N)[N] Y

This command will reset the whole system and disconnect your current session. Reload is scheduled for 17:12:00 UTC Wed Jun 6 2012 (in 34 minutes). Do you want to continue? (Y/N)[N] Y

06-Jun-2012 16:37:18 %RNDMISC-N-SRACTIVE: system is scheduled to perform a restart at 17:12:00 Wed Jun 6 2012 (in 34 minutes).

Example 4—The following example cancels a reload.

switchxxxxxx# reload cancel

Reload cancelled.

5.7 show reload

The show reload Privileged EXEC mode command displays whether there is a pending reload for the device.

Syntax

show reload

Parameters

N/A
Default Usage
N/A

Command Mode
Privileged EXEC mode

User Guidelines
You can use this command to display a pending software reload. To cancel a pending reload, use the privileged EXEC command with the cancel parameter.

Example
The following example displays that a reboot is scheduled for 00:00 on Saturday, April-20.

```
switchxxxxxx# show reload
Reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
or
Scheduled reload is not configured.
```

5.8 service cpu-utilization
The service cpu-utilization Global Configuration mode command enables measuring CPU utilization. Use the no form of this command to restore the default configuration.

Syntax
```
service cpu-utilization
no service cpu-utilization
```

Parameters
N/A

Default Configuration
Measuring CPU utilization is disabled.
Command Mode
Global Configuration mode

User Guidelines
Use the **service cpu utilization** command to measure information on CPU utilization.

Example
The following example enables measuring CPU utilization.

```
switchxxxxxx(config)# service cpu-utilization
```

### 5.9 show cpu utilization

The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

Syntax
```
show cpu utilization
```

Parameters
N/A

Default Usage
N/A

Command Mode
Privileged EXEC mode

User Guidelines
Use the **show cpu-utilization** command to enable measuring CPU utilization.

Example
The following example displays CPU utilization information.
switchxxxxxxx# **show cpu utilization**

CPU utilization service is on.

CPU utilization

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

five seconds: 5%; one minute: 3%; five minutes: 3%

### 5.10 show users

The **show users** EXEC mode command displays information about the active users.

**Syntax**

`show users`

**Parameters**

N/A

**Default Usage**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays information about the active users.

```
switchxxxxxxx# **show users**

Username  Protocol  Location
----------  --------  --------
Bob        Serial    
John       SSH       172.16.0.1
Robert     HTTP      172.16.0.8
Betty      Telnet    172.16.1.7
Sam        172.16.1.6
```
5.11 show sessions

The `show sessions` EXEC mode command displays open Telnet sessions.

Syntax

```
show sessions
```

Parameters

N/A

Default Usage

N/A

Command Mode

EXEC mode

User Guidelines

The `show sessions` command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.

Example

The following example displays open Telnet sessions.

```
switchxxxxxx# show sessions
```

<table>
<thead>
<tr>
<th>Connection</th>
<th>Host</th>
<th>Address</th>
<th>Port</th>
<th>Byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote router</td>
<td>172.16.1.1</td>
<td>23</td>
<td>89</td>
</tr>
<tr>
<td>2</td>
<td>172.16.1.2</td>
<td>172.16.1.2</td>
<td>23</td>
<td>8</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown above.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>The connection number.</td>
</tr>
<tr>
<td>Host</td>
<td>The remote host to which the device is connected through a Telnet session.</td>
</tr>
</tbody>
</table>
The `show system` EXEC mode command displays various items of information about the device.

**Syntax**

```
show system
```

**Parameters**

N/A.

**Command Mode**

EXEC mode

**Example**

```
switchxxxxxx# show system
System Description: 20-port Gigabit Managed Switch
System Up Time (days,hour:min:sec): 03,02:27:46
System Contact:
System Name: switch151400
System Location:
System MAC Address: 00:24:ab:15:14:00
System Object ID: 1.3.6.1.4.1.9.6.1.83.20.1
Main Power Supply Status: OK
Fans Status: OK
```

### 5.12 show version

The `show version` EXEC mode command displays system version information.

**Syntax**

```
show version
```

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The remote host IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The Telnet TCP port number.</td>
</tr>
<tr>
<td>Byte</td>
<td>The number of unread bytes for the user to see on the connection.</td>
</tr>
</tbody>
</table>
Parameters

Default Usage
N/A

Command Mode
EXEC mode

Example
The following example displays system version information.

```bash
switchxxxxxxx# show version
SW Version 1.1.0.5 ( date 15-Sep-2010 time 10:31:33 )
Boot Version 1.1.0.2 ( date 04-Sep-2010 time 21:51:53 )
HW Version V01
```

5.13 show environment

This command is only relevant for devices that have temperature sensors.

The show environment EXEC mode command displays environment information.

Syntax
```
show environment {all | fan | temperature {status} }
```

Parameters
- **all** —Displays the fan and temperature general status
- **fan** —Displays the fan status
- **temperature status** —Displays the temperature status
Command Mode
EXEC mode

User Guidelines
The fan and temperature status parameters are available only on devices on which FAN and/or temperature sensor are installed.

Examples
Example 1 - The following example displays the general environment status of a device
The temperature status is OK if the temperature sensors status in the device is OK, and if the temperature of all the device is below the threshold.

switchxxxxxx # show environment all
FAN is OK
TEMPERATURE is OK

Example 2 - The following example displays the general FAN status of a device.
switchxxxxxx # show environment fan
FAN is OK

Example 3 - The following example displays the detailed temperature status of a device
switchxxxxxx # show environment temperature status
TEMPERATURE is OK

5.14 show version md5
Use the show version md5 EXEC mode command to display external MD5 digest of firmware.

Syntax
show version md5
Parameters

Default Usage
N/A

Command Mode
EXEC mode

Example

switchxxxxxx# show version md5
Filename Status MD5 Digest
-------- ------- ----------------------------------
image1 Active 23FA000012857D8855AABC7577AB5562
image2 Not Active 23FA000012857D8855AABEA7451265456
boot 23FA000012857D8855AABC7577AB8999
image1 Not Active 23FA000012857D8855AABC7577FE693844
image2 Active 23FA000012857D8855AABC7577AB5562
boot 23FA000012857D8855AABC7577AC9999

5.15 set system

The **set system** Privileged EXEC mode command puts the device into switch mode (Layer 2 mode) or router mode (Layer 3 mode).

Syntax

set system mode **{router / switch}**

Parameters **{router / switch}**

- **router**—Specifies that the device functions as a switch-router.
- **switch**—Specifies that the device functions as a switch.

Default Configuration

The default configuration is switch mode (Layer 2).
Command Mode

Privileged EXEC mode

User Guidelines

The System mode appears in the configuration file header to specify the system mode. It appears even if it specifies the default system mode.

If this command is entered manually and the configured system mode does not match the current system mode, the Startup Configuration file is deleted and the device is rebooted. It is highly recommended to back up the Startup Configuration file before executing this command; otherwise the device is configured in the new system mode with an empty configuration.

If the system mode is contained in a configuration file that is downloaded to the device, but the file’s system mode matches the current system mode, this information is ignored. Otherwise the following cases occurs:

- If this file is copied manually onto the device (using copy tftp, for example), the operation is aborted, and a message is displayed indicating that the system mode must be changed manually.

- If this file is downloaded during the automatic configuration process, the Startup Configuration file is deleted and the device reboots automatically in the new system mode and the device is configured with an empty configuration.

Example

The following example configures the device to function as a switch-router (Layer 3).

```
switchxxxxxx# set system mode router
```

5.16 show system mode

The **show system mode** EXEC mode command displays information on features control.

Syntax

```
show system mode
```
Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

Example
The following example displays system mode information.

```
switchxxxxxx# show system mode
Feature     State
-------------------     ---------
Mode:             Router
```

5.17  **show system languages**

The **show system languages** EXEC mode command displays the list of supported languages.

Syntax

```
show system languages
```

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode
Example
The following example displays the languages configured on the device. Number of Sections indicates the number of languages permitted on the device.

```
switchxxxxxx# show system languages
Language Name     Unicode Name   Code   Num of Sections
--------------- -------------- ------ --------------
  English         English     en-US   2
  Japanese        µùѵ£¼F¬P   ja-JP   2
```

5.18 show system tcam utilization
The `show system tcam utilization` EXEC mode command displays the Ternary Content Addressable Memory (TCAM) utilization.

Syntax
```
show system tcam utilization
```

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

Example
The following example displays TCAM utilization information.

```
switchxxxxxx# show system tcam utilization
TCAM utilization: 58%
```
5.19 show services tcp-udp

Use the show services tcp-udp Privileged EXEC mode command to display information about the active TCP and UDP services.

Syntax

show services tcp-udp

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

The output does not show sessions where the device is a TCP/UDP client.

Examples

```
switchxxxxxx# show services tcp-udp
Type  Local IP Address  Remote IP address  Service Name  State
---------------------- ------------------- ------------- ----------
TCP     All:22           SSH               LISTEN
TCP     All:23           Telnet            LISTEN
TCP     All:80           HTTP              LISTEN
TCP     All:443          HTTPS             LISTEN
TCP     172.16.1.1:23    172.16.1.18:8789  Telnet         ESTABLISHED
TCP6    All-23           Telnet            LISTEN
TCP6    fe80::200:b0ff:fe00:0-23 fe80::200:b0ff:fe00:0-8999 Telnet         ESTABLISHED
UDP     All:161          SNMP             
UDP6A   11-161           SNMP              
```
5.20  show tech-support

Use the show tech-support EXEC mode command to display system and configuration information that can be provided to the Technical Assistance Center when reporting a problem.

Syntax

show tech-support [config] [memory]

Parameters

- Memory—Displays memory and processor state data.
- Config—Displays switch configuration within the CLI commands supported on the device.

Default Configuration

By default, this command displays the output for technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Types

Switch command.

Command Mode

EXEC mode

User Guidelines

Caution: Avoid running multiple show tech-support commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The show tech-support command may timeout if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a set logout timeout value of 0 to disable automatic disconnection of idle sessions or enter a longer timeout value.

The show tech-support command output is continuous, it does not display one screen at a time. To interrupt the output, press Esc.
If you specify the `config` keyword, the `show tech-support` command displays the output of the following commands (depending on the commands supported on the device):

- `show clock`
- `show system`
- `show version`
- `show system mode`
- `show ip interface`
- `show ipv6 interface`
- `show running-config`
- `show interfaces configuration`
- `show interfaces status`
- `show interfaces port-channel`
- `show vlan`
- `show interfaces switchport`
- `show bridge multicast address-table`
- `show spanning tree`
- `show ip igmp snooping groups`
- `show ipv6 mld snooping groups`
- `show dot1x`
- `show dot1x users`
- `show lldp configuration`
- `show lldp neighbors`
- `show errdisable interface`
- `show interfaces counters`
- `show power inline`
- `show cdp`
- `show cdp traffic global`
- show cdp traffic
- show cdp neighbors
- show voice vlan
- show users
- show sessions
- show logging file
- show logging

If the user specifies the memory keyword, the show tech-support command displays the following output:

- Flash info (dir if existed, or flash mapping)
- Output of command show bootvar
- Buffers info (like print os buff)
- Memory info (like print os mem)
- Proc info (like print os tasks)
- Versions of software components
- Output of command show cpu utilization

### 5.21 show system id

The `show system id` EXEC mode command displays the system identity information.

**Syntax**

`show system id`

**Parameters**

N/A.

**Command Mode**

EXEC mode
Example
The following example displays the system identity information.

```
switchxxxxxx# show system id
serial number 114
```

5.22 show cpu input rate
The show cpu input rate EXEC mode command displays the rate of input frames to the CPU in packets per seconds (pps).

Syntax
show cpu input rate

Command Mode
EXEC mode

Example
The following example displays CPU input rate information.

```
switchxxxxxx# show cpu input rate
Input Rate to CPU is 1030 pps.
```

5.23 menu
The menu EXEC mode command opens the boot menu.

Syntax
menu

Command Mode
EXEC mode

Example
5.24  disable ports leds

Use the disable ports leds Global Configuration mode command to turn off the LEDs of all the ports on a device (depending on the actual port status, e.g. link up, port speed etc).

Use no disable ports leds command to set the LEDs of all the ports on the device to their current operational status.

Syntax

disable ports leds

no disable ports leds

Parameters

N/A

Default Configuration

The default is no disable port leds; that is the LEDs of all the ports reflect their current status

Command Mode

Global Configuration mode

User Guidelines

N/A

Examples

The following example turns off the port LEDs.

switchxxxxxx# disable ports leds

5.25  show ports leds configuration

Use the show ports leds configuration EXEC mode command to display whether the LEDs of all the ports are enabled or disabled.
System Management Commands

Syntax
show ports leds configuration

Command Mode
EXEC mode

Examples
Example 1 - The following example displays the status of the ports LEDs when the port LEDs are turned on.
show ports leds configuration
Port leds are not disabled

Example 2: The following example displays the status of the ports LEDs when the port LEDs are turned off.
show ports leds configuration
Port leds are disabled

5.26 show system fans

Use the show system fans EXEC mode command to view the status of the fans on the device.

Syntax
show system fans

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode
Example

If the device does not support controlled fan direction, the column Fan Direction is not displayed.

```
switchxxxxxx# show system fans
Unit  Speed     Admin State   Oper State  Fan Direction
      (RPM)               
---  --------  -----------  -----------  --------------
1     0       auto OK       back to front
```

5.27  show system sensors

Use the `show system sensors` EXEC mode command to view the temperature sensor status of the device.

Syntax

```
show system sensors
```

Parameters

N/A

Default Usage

N/A

Command Mode

EXEC mode

Examples

```
switchxxxxxx# show system sensors
Sensor Status: OK
Temperature(C): 37
```
5.28  system recovery

This command is only relevant for devices that have temperature sensors.

Use the `system recovery` Global Configuration command to set the system to automatically recover from temperature that reached the critical threshold.

Use the `no` form of the command to return to disable automatic recovery.

**Syntax**

```
system recovery
no system recovery
```

**Parameters**

N/A

**Default Configuration**

System recovery is enabled by default.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# no system recovery
```
6.1 ip ssh-client authentication

Use the ip ssh-client authentication command in Global Configuration mode to define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers.

To return to default, use the no format of the command.

**Syntax**

```
ip ssh-client authentication {password | public-key {rsa | dsa}}
no ip ssh-client authentication
```

**Parameters**

- **password**— Username and password are used for authentication.
- **public-key rsa**— Username and RSA public key are used for authentication.
- **public-key dsa**— Username and DSA public key are used for authentication.

**Default Configuration**

Username and password are used for authentication by the local SSH clients.

**Command Mode**

Global Configuration

**User Guidelines**

A user can use the ip ssh-client key command to generate/configure RSA/DSA keys if SSH authentication is by public key. Otherwise, the default keys generated by the switch are used.
Example
The following example specifies that, username and public key are used for authentication:

```
switchxxxxxx(config)# ip ssh-client authentication public-key rsa
```

### 6.2 ip ssh-client change server password

Use the `ip ssh-client change server password` command in Global Configuration mode to change a password of an SSH client on a remote SSH server.

**Syntax**

```
ip ssh-client change server password server {host | ip-address | ipv6-address} username username old-password old-password new-password new-password
```

**Parameters**

- **host** — DNS name of a remote SSH server.
- **ip-address** — Specifies the IP address of a remote SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **username** — Username of the local SSH clients (1 - 70 characters).
- **old-password** — Old password of the local SSH client (1 - 70 characters).
- **new-password** — New password for the local SSH client (1 - 70 characters). The password cannot include the characters "@" and ":".

**Default Configuration**

N/A

**Command Mode**

Global configuration

**User Guidelines**

Use the command to change a password on a remote SSH server. Use `ip ssh-client password` to change the SSH client password of the switch’s SSH client so that it matches the new password set on the remote SSH server.
Example

The following example changes a password of the local SSH clients:

```bash
switchxxxxxx(config)# ip ssh-client change server password server 10.7.50.155
username john old-password &&&@@@aaff new-password &&&@@@aaee
```

### 6.3 ip ssh-client key

Use the `ip ssh-client key` command in Global Configuration mode to create a key pair for SSH client authentication by public key (either by generating a key or by importing a key). To enter the private key as encrypted, use the `encrypted ip ssh-client key` command.

To remove a key, use the `no` form of the command.

**Syntax**

```
ip ssh-client key {dsa | rsa} {generate | key-pair privkey pubkey}
encrypted ip ssh-client key {dsa | rsa} key-pair encrypted-privkey pubkey
no ip ssh-client key [dsa | rsa]
```

**Parameters**

- `dsa`—DSA key type.
- `rsa`—RSA key type.
- `key-pair`—Key that is imported to the device.
- `privkey`—Plaintext private key.
- `encrypted-privkey`—Private key is in encrypted format.
- `pubkey`—The plaintext public key.

**Default Configuration**

The application creates a key automatically, which is the default key.

**Command Mode**

Global configuration
User Guidelines

When using the keyword **generate**, a private key and a public key of the given type (RSA/DSA) are generated for the SSH client. Downloading a configuration file with a Key Generating command is not allowed, and such download will fail.

When using the keyword **key-pair**, the user can import a key-pair created by another device. In this case, the keys must follow the format specified by RFC 4716.

If the specified key already exists, a warning will be issued before replacing the existing key with a new key.

Use the **no ip ssh-client key** command to remove a key pair. Use this command without specifying a key-type to remove both key pairs.

**Table 3** describes the expected behavior of keys, default and users within the various operations.

<table>
<thead>
<tr>
<th>From/To</th>
<th>Show</th>
<th>Show (detailed)</th>
<th>Copy/Upload of Running Config</th>
<th>Copy/Upload of Startup Config</th>
<th>Download text-based CLI (TFTP/Backup)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Config</td>
<td>Only user-defined.</td>
<td>N/A</td>
<td>All keys (default and user)</td>
<td>N/A</td>
<td>All keys (default and user)</td>
</tr>
<tr>
<td>Running Config</td>
<td>Keys are not displayed.</td>
<td>All keys (default and user)</td>
<td>N/A</td>
<td>Only user defined.</td>
<td>Same as user configuration</td>
</tr>
<tr>
<td>Text-based CLI</td>
<td>As it was copied.</td>
<td>N/A</td>
<td>All keys (default and user)</td>
<td>Only user defined.</td>
<td>As a text file.</td>
</tr>
</tbody>
</table>

If no keys are included in text-based configuration file, the device generates it’s own keys during initialization. If the Running Configuration contains default keys (not user-defined), the same default keys remain.

Examples

**Example 1** - In the following example, a key pair of the RSA type is created:

```
switchxxxxxx(config)# ip ssh-client key rsa generate
```

The SSH service is generating a private RSA key.
This may take a few minutes, depending on the key size.

**Example 2.** In the following example, both public and private keys of the RSA type are imported (private key as plaintext):

```
switchxxxxxx(config)#ip ssh-client key rsa key-pair
```

Please paste the input now, add a period (.) on a separate line after the input

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CU/2KYR18rYrK5+TIvwS4zvhBmiC4i31m9cR/1iRTFV1MRuJ++Te
p9ssqWyI1T19d0jzmGON3jHzp2je5/DUTHZXvYaUzchBDnsFTJo8dyiB14YbqYHqCjUhk
tXqvloy+1uxRJTAalVXCBAmuIU/kMLoEox8/zwJB/jsF9wIBiVBgC2xZ5mQmvy0+yo2GU
FwlQO5f0yweuM11J8McTmqDgfVTRrdbroXwbs3exVqsfalUPY9wa8Le6JPX+Dp4XovEfC/
ig1ZBSC8SeDmI2U7D6HrkAyD9HHf/r32jukB+527B1HPz2Xczs2c100wryToy+YTzjLUxy
WS7V/Ixb1liplAKeA/QlVSCfFmdM1ixaEfJVzqP01cF8guwsWLteBf/gqHuvbHuNy0t
OWEpObKZs1m/mtCWppkgcqrgrBo0JaYbUFQJBAMo/cCrkyhsIV/+ZsryeD26NhBEKiaak16V
Tz2ayDstatGuuvcvm2YF7djM6n6NYz3+/2Lyc5n82okb1dINhDONsCQQMcxaas+C4HaHqns
zSU/+1W1D188As4qjN2DMmGJbtbSHhQxWIHAG4tBVWa8bV12+RPyuwan/jnk8irniGyVza
FPakEAlq8oV+1XYx8V39V/a42d7FvRjMckUmK14Rmt32+u9i6sFzaWcdgs87+2vS3AZQ
afqDE5U6YSMiGLVewC4YWwJBAOFZmhO+d1lxT8Irzf2cUZggopfnX6Y+lY109MuZHbwH
TXaBGj6ayMYvXnzOcNecnApBjGEm37YVwKj02DV2w=
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMfoJT/YphGyxtisrn5M1/BLjo+EGaILgjfWb1xH/WJFVMWixG4n75bSun2yyp
BIjYOL13SFOyB3eMfOnaN7n8HMsb89hpTNYeEOew9Mmjx3KIGXhgGpdCAKNSG51eq+W
jl7W7FeLMBotVcIECa4hT+QwugSjHz/FCMH+CwX3AgBj
-----END RSA PUBLIC KEY-----
```


**Example 3.** In the following example, both public and private keys of the DSA type are imported (private key as encrypted):

```
switchxxxxxx(config)# encrypted ip ssh-client key rsa key-pair
```
(Need to encrypted SSH client RSA key pair, for example:)

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
gxeOjs6OzGRtL4qstnQq1B/4gexQb1fa56RdjgHAMejvUT02e1YmNi+m4aTu6mlvXPHmY
1X1Xmy7jZkHRvgg8EzcppEB003yQzq3kNi756cMg4Oqbkm7TU0tdqYFEz/h8rJJOvUFfh
BsEQ3e16E/OPitWgK43WtzedsuPyFeOoMXR9BCuxPUJuCd2UeqQVM21Jt5OM0FbVt0S6ogXhG
sEEdoT1h1DwHWg97Fcv7x+bEnPfzFGmrbrUxcxOx1kPsUNo3/94PHK8zEXyWtrx2KoCDQ
qFRuM8uecpjmDb6MO2GURVstctohEWEIVCIOr5SBCbciaxv5oS0jIzXMrJAn
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALLOeh3css8tBL8ujFt3trcX0XJyJlxxxt4sGp8Q3Ex1SRN25+Mcac6t0gpIEg
tIk6tIIEJscuAh9Brwh1ovgMLRaMe25j5Yj04xG6Fp42nhHiRcie+YTS1o309EdZkixa
QeJtldnYL/r3uTIRVGbXI5nxwtfWpwExgxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----
```

Example 4 - In the following example, a DSA key pair is removed:

```
switchxxxxxx(config)# no ip ssh-client key dsa
```

Example 5 - In the following example, all key pairs (RSA and DSA types) are removed.

```
switchxxxxxx(config)# no ip ssh-client key
```

### 6.4 ip ssh-client password

Use the `ip ssh-client password` command in Global Configuration mode to configure the password for SSH client authentication by password. To enter the password as encrypted, use the `encrypted ip ssh-client password` command.

To return to default, use the `no` form of the command.

**Syntax**

```
ip ssh-client password string
encrypted ip ssh-client password encrypted-string
```
no ip ssh-client password

Parameters

- **string**— Password for the SSH clients (1 - 70 characters). The username cannot include the characters "@" and ":".

- **encrypted-string** - Password for the SSH client in encrypted form.

Default Configuration

The default password is anonymous.

Command Mode

Global configuration

User Guidelines

The password cannot include the characters "@" and ":".

If authentication is configured to use a password (using the command `ip ssh-client authentication`), use the `ip ssh-client password` command to define the password.

If the encrypted key-word is used, the password must be in the encrypted form.

Use the command `ip ssh-client change server password` to change the password on the remote SSH server so that it will match the new password of the SSH client.

Example

The following example specifies a plaintext password for the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client password &&&111aaff
```

### 6.5 ip ssh-client server authentication

Use the `ip ssh-client server authentication` command in Global Configuration mode to enable remote SSH server authentication by the SSH client.

To disable remote SSH server authentication, use the `no` form of the command.

**Syntax**

ip ssh-client server authentication
no ip ssh-client server authentication

Parameters
None

Default Configuration
SSH server authentication is disabled

Command Mode
Global configuration

User Guidelines
When remote SSH server authentication is disabled, any remote SSH server is accepted (even if there is no entry for the remote SSH server in the SSH Trusted Remote Server table).

When remote SSH server authentication is enabled, only trusted SSH servers are accepted. Use the `ip ssh-client server fingerprint` command to configure trusted SSH servers.

Example
The following example enables SSH server authentication:

```
switchxxxxxx(config)# ip ssh-client server authentication
```

### 6.6 ip ssh-client server fingerprint

Use the `ip ssh-client server fingerprint` command in Global configuration mode to add a trusted server to the Trusted Remote SSH Server Table. To remove an entry or all entries from the Trusted Remote SSH Server Table, use the `no` form of the command.

Syntax

```
ip ssh-client server fingerprint {host | ip-address} fingerprint

no ip ssh-client server fingerprint [host | ip-address]
```

Parameters

- `host`—DNS name of a SSH server.
- **ip-address**—Specifies the address of a SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

- **fingerprint**—Fingerprint of the SSH server public key (32 Hex characters).

**Default Configuration**

The Trusted Remote SSH Server table is empty.

**Command Mode**

Global configuration

**User Guidelines**

Fingerprints are created by applying a cryptographic hash function to a public key. Fingerprints are shorter than the keys they refer to, making it simpler to use (easier to manually input than the original key). Whenever the switch is required to authenticate an SSH server’s public key, it calculates the received key’s fingerprint and compares it to the previously-configured fingerprint.

The fingerprint can be obtained from the SSH server (the fingerprint is calculated when the public key is generated on the SSH server).

The `no ip ssh-client server fingerprint` command removes all entries from the Trusted Remote SSH Server table.

**Example**

In the following example, a trusted server is added to the Trusted Servers table (with and without a separator ":"):  

```
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1  DC789788DC88A988127897BCBB789788
```

**6.7 ip ssh-client username**

Use the `ip ssh-client username` command in Global Configuration mode to configure the SSH client username of the switch.

To return to default, use the `no` form of the command.
SSH Client Commands

Syntax

ip ssh-client username string

no ip ssh-client username

Parameters

string— Username of the SSH client. The length is 1 - 70 characters. The username cannot include the characters "@" and ":".

Default Configuration

The default username is anonymous

Command Mode

Global configuration

User Guidelines

The username cannot include the characters "@" and ":".

The configured username is used when SSH client authentication is done both by password or by key.

Example

The following example specifies a username of the SSH client:

```
switchxxxxxx(config)# ip ssh-client username jeff
```

6.8 show ip ssh-client

Use the show ip ssh-client command in Privilege EXEC mode to display the SSH client credentials, both default and user-defined keys.

Syntax

show ip ssh-client

show ip ssh-client {mypubkey | key} {dsa | rsa}

Parameters

- dsa— Specifies displaying the DSA key type.
SSH Client Commands

- `rsa`— Specifies displaying the RSA key type.
- `mypubkey`— Specifies that only the public key is selected to be displayed.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use the command with a specific key-type to display the SSH client key; You can either specify display of public key or private key, or with no parameter to display both private and public keys. The keys are displayed in the format specified by RFC 4716.

**Examples**

**Example 1** - The following example displays the authentication method and the RSA public key:

```bash
switchxxxxxx# show ip ssh-client mypubkey rsa
```

Authentication method: RSA key
Username: John
Key Source: User Defined

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIAwAAAIEAss56Hdyyzy0Evyy6MW3e2txfRcnIkuXHG3iwanxDcTGVJE3bn4xpxpq2iCkgSCOjOTq3UgOmx4CKHGvCHWiAwtFox7bmPlIM7jEboWnjaeeJFyJ75hNLWjfT0RlmSdpB4m0t2dgy+ve5MhFU2tcj
mfHC19anASDHEPB+rMc=

---- END SSH2 PUBLIC KEY ----
```


**Example 2.** The following example displays the authentication method and DSA private key in encrypted format:

```bash
switchxxxxxx# show ip ssh-client key DSA
```

Authentication method: DSA key
Username: john
Key Source: User Defined

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACABAFY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rz2dzoSOXxbET
W6ToHv8D1UJ/8+zHo9Fiko5XybZnDIAbDHt1bLQ+yP7Stxy1tHnXF1YLFKDLG4T6JYrdH
YI14Omleg9e4NhCRlea0g2PF3UGFzi6bXrGTQf3gJq2e7Yisk/gF+fVAAAAAFQdb8D5c
vwHTZDPFx0D2s9Rd7NBvQAAAIEA1N92+Bb7D4KLYK3IrRbxb1wXdkPGgA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6txWxYN7PK5SR/FXPnxwHPapc9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuM0EsSNhVDTx3WdVscBq9cetztroKtW0ocJmJ80qadxTRHtUAACAB
AN7CY+Kv1gHPrzFwdQm7HK9b1bLAoZKwaoXnadFgeptNBQeSEXG1v0+JsvphVMBC9HS
n24VYtYsMu74qXv1YziVucWKjjKE11juqnF0GD1B3VVmxHLMnxAz643WK4227dLM5
sY29ouezv4Xz2PuMch5VGFP+CdquizCM41oWgV

---- END SSH2 PUBLIC KEY ----

---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACABAFY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rz2dzoSOXxbET
W6ToHv8D1UJ/8+zHo9Fiko5XybZnDIAbDHt1bLQ+yP7Stxy1tHnXF1YLFKDLG4T6JYrdH
YI14Omleg9e4NhCRlea0g2PF3UGFzi6bXrGTQf3gJq2e7Yisk/gF+fVAAAAAFQdb8D5c
vwHTZDPFx0D2s9Rd7NBvQAAAIEA1N92+Bb7D4KLYK3IrRbxb1wXdkPGgA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6txWxYN7PK5SR/FXPnxwHPapc9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuM0EsSNhVDTx3WdVscBq9cetztroKtW0ocJmJ80qadxTRHtUAACAB
AN7CY+Kv1gHPrzFwdQm7HK9b1bLAoZKwaoXnadFgeptNBQeSEXG1v0+JsvphVMBC9HS
n24VYtYsMu74qXv1YziVucWKjjKE11juqnF0GD1B3VVmxHLMnxAz643WK4227dLM5
sY29ouezv4Xz2PuMch5VGFP+CdquizCM41oWgV

---- END SSH2 PRIVATE KEY ----

**Example 3.** The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
```
Authentication method: password (default)
Username: anonymous (default)
password(Encrypted): KzGgpvYa7GzCHhaveSJDehGJ6L3Yf92BAU5nsxSwic=

6.9 show ip ssh-client server

Use the show ip ssh-client server command in Privilege EXEC Configuration mode to display the SSH remote server authentication method and the Trusted Remote SSH Server table.

Syntax

show ip ssh-client server [host | ip-address]

Parameters

- host — DNS name of an SSH server.
- ip-address — IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

N/A

Command Mode

Privilege EXEC configuration mode

User Guidelines

If a specific SSH server is specified, only the fingerprint of this SSH server is displayed. Otherwise, all known servers are displayed.

Examples

Example 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:

```
switchxxxxxx# show ip ssh-client server
SSH Server Authentication is enabled
server address: 11.1.0.1
```
server address: 192.165.204.111

server address: 4002:0011::12

Clock Commands

7.1 clock set

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

Syntax

clock set hh:mm:ss [[day month] | [month day]] year

Parameters

- **hh:mm:ss**—Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)
- **day**—Specifies the current day of the month. (Range: 1-31)
- **month**—Specifies the current month using the first three letters of the month name. (Range: Jan–Dec)
- **year**—Specifies the current year. (Range: 2000–2037)

Command Mode

Privileged EXEC mode

User Guidelines

It is recommended that the user enter the local clock time and date.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
switchxxxxxx# clock set 13:32:00 7 Mar 2005
```

7.2 clock source

The clock source Global Configuration mode command configures an external time source for the system clock. Use the no form of this command to disable the external time source.
Clock Commands

7.3 clock timezone

Use the clock timezone Global Configuration command to set the time zone for display purposes. Use the no form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.

Syntax

clock timezone zone hours-offset [minutes-offset]

no clock timezone

Parameters

• sntp—Specifies that an SNTP server is the external clock source.

• browser—Specifies that if the system clock is not already set (either manually or by SNTP) and a user logs on to the device using a WEB browser (either via HTTP or HTTPS), the system clock will be set according to the browser’s time information.

Default Configuration

There is no external clock source.

Command Mode

Global Configuration mode

Example

The following example configures an SNTP server as an external time source for the system clock.

switchxxxxxx(config)# clock source sntp

7.3 clock timezone

Use the clock timezone Global Configuration command to set the time zone for display purposes. Use the no form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.

Syntax

clock timezone zone hours-offset [minutes-offset]

no clock timezone

Parameters

• sntp—Specifies that an SNTP server is the external clock source.

• browser—Specifies that if the system clock is not already set (either manually or by SNTP) and a user logs on to the device using a WEB browser (either via HTTP or HTTPS), the system clock will be set according to the browser’s time information.

Default Configuration

There is no external clock source.

Command Mode

Global Configuration mode

Example

The following example configures an SNTP server as an external time source for the system clock.

switchxxxxxx(config)# clock source sntp
Parameters

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

Default Configuration

Offsets are 0.
Acronym is empty.

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
```

7.4 **clock summer-time**

Use one of the formats of the **clock summer-time** Global Configuration command to configure the system to automatically switch to summer time (Daylight Saving Time). Use the **no** form of this command to configure the software not to automatically switch to summer time.

Syntax

- `clock summer-time zone recurring {usa | eu} [week day month hh:mm week day month hh:mm] [offset]`
- `clock summer-time zone date day month year hh:mm date month year 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 summer time is in effect. (Range: up to 4 characters)
- **recurring**—Indicates that summer time starts and ends on the corresponding specified days every year.
- **date**—Indicates that summer time starts on the first date listed in the command and ends on the second date in the command.
- **usa**—The summer time rules are the United States rules.
- **eu**—The summer time rules are the European Union rules.
- **week**—Week of the month. Can be 1–4, first, last.
- **day**—Day of the week (first three characters by name, such as Sun).
- **date**—Date of the month. (Range: 1–31)
- **month**—Month (first three characters by name, such as Feb).
- **year**—Year (no abbreviation). (Range: 2000–2097)
- **hh:mm**—Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- **offset**—Number of minutes to add during summer time (default is 60). (Range: 1440)

Default Configuration

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 summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.
USA rules for Daylight Saving Time:

- From 2007:
  - Start: Second Sunday in March
  - End: First Sunday in November
  - Time: 2 AM local time
- Before 2007:
  - Start: First Sunday in April
  - End: Last Sunday in October
  - Time: 2 AM local time

EU rules for Daylight Saving Time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

Example

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

7.5  **clock dhcp timezone**

Use the `clock dhcp timezone` Global Configuration command to specify that the timezone and the Summer Time (Daylight Saving Time) of the system can be taken from the DHCP Timezone option. Use the `no` form of this command disable this option.

**Syntax**

```
clock dhcp timezone
no clock dhcp timezone
```

**Parameters**

N/A
Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
The TimeZone taken from the DHCP server has precedence over the static TimeZone. If the TimeZone does not exist in the DHCP-TimeZone option, the static configuration will be active.

The Summer Time taken from the DHCP server has precedence over static SummerTime. If the Summer Time does not exist in the DHCP-TimeZone option, the static configuration will be active.

The TimeZone and SummerTime remain effective after the IP address lease time has expired.

The TimeZone and SummerTime that are taken from the DHCP server are cleared after reboot.

When the user disables taking the TimeZone and Summer Time from the DHCP server, the dynamic Time Zone and Summer Time from the DHCP server are cleared.

In case of multiple DHCP-enabled interfaces, the last accepted DHCP-Time Zone option overrides any previous DHCP-Time Zone option. This means that the last accepted DHCP-Time Zone option overrides the previous Time Zone and the Summer Time, even if it includes only one of them.

Disabling the DHCP client from where the DHCP-TimeZone option was taken, clears the dynamic Time Zone and Summer Time configuration.

Example

```
switchxxxxx(config)# clock dhcp timezone
```

7.6 sntp authentication-key

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

sntp authentication-key key-number md5 key-value
encrypted sntp authentication-key key-number md5 encrypted-key-value
no sntp authentication-key key-number

Parameters

- **key-number**—Specifies the key number. (Range: 1–4294967295)
- **key-value**—Specifies the key value. (Length: 1–8 characters)
- **encrypted-key-value**—Specifies the key value in encrypted format.

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

Examples

The following example defines the authentication key for SNTP.

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

7.7 **sntp authenticate**

The **sntp authenticate** Global Configuration mode command enables authentication for received SNTP traffic from servers. Use the **no** form of this command to disable the feature.

Syntax

sntp authenticate

no sntp authenticate
Parameters
N/A

Default Configuration
Authentication is disabled.

Command Mode
Global Configuration mode

User Guidelines
The command is relevant for both Unicast and Broadcast.

Examples
The following example enables authentication for received SNTP traffic and sets the key and encryption key.

```
snpp authenticate
snpp authentication-key 8 md5 ClkKey
snpp trusted-key 8
```

7.8  **snpp trusted-key**

The **snpp trusted-key** Global Configuration mode command authenticates the identity of the system with which SNTP synchronizes. Use the **no** form of this command to disable system identity authentication.

Syntax

```
snpp trusted-key key-number
no snpp trusted-key key-number
```

Parameters

```
key-number—Specifies the key number of the authentication key to be trusted. (Range: 1–4294967295)
```
Default Configuration
No keys are trusted.

Command Mode
Global Configuration mode

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

Examples
The following example authenticates key 8.

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

7.9  sntp broadcast client enable
The sntp broadcast client enable Global Configuration mode command enables SNTP Broadcast clients. Use the no form of this command to disable SNTP Broadcast clients.

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

Default Configuration
The SNTP Broadcast client is disabled.

Command Mode
Global Configuration mode
User Guidelines

Use the `sntp broadcast client enable` Interface Configuration mode command to enable the SNTP Broadcast client on a specific interface.

After entering this command, you must enter `clock source snmp` for the command to be run. If this command is not run, the switch will not synchronize with Broadcast servers.

Example

The following example enables SNTP Broadcast clients.

```
switchxxxxxx(config)# sntp broadcast client enable
```

7.10 `sntp anycast client enable`

The `sntp anycast client enable` Global Configuration mode command enables the SNTP Anycast client. Use the `no` form of this command to disable the SNTP Anycast client.

Syntax

```
sntp anycast client enable
no sntp anycast client enable
```

Parameters

N/A

Default Configuration

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enable the SNTP Anycast client.
Example
The following example enables SNTP Anycast clients.

```
switchxxxxxx(config)# sntp anycast client enable
```

### 7.11 sntp client enable

The `sntp client enable` Global Configuration mode command enables the SNTP Broadcast and Anycast client on an interface when the device is in Router mode (Layer 3). Use the `no` form of this command to disable the SNTP Broadcast and Anycast client.

**Syntax**

```
sntp client enable {interface-id}
no sntp client enable {interface-id}
```

**Parameters**

- `interface-id`—Specifies an interface ID, which can be one of the following types: Ethernet port, Port-channel or VLAN.

**Default Configuration**

The SNTP client is disabled on an interface.

**Command Mode**

Global Configuration mode - Ethernet port, Port-channel or VLAN.

**User Guidelines**

This command only works when the device is in Router mode (Layer 3).

The `sntp broadcast client enable` Global Configuration mode command globally enables Broadcast clients.

This command enables both.
### Example

The following example enables the SNTP Broadcast and Anycast client on port gi3.

```text
switchxxxxxx(config)# sntp client enable gi3
```

#### 7.12 sntp client enable (Interface)

To enable the SNTP Broadcast and Anycast client on an interface, use the `sntp client enable` Interface Configuration command. Use the `no` form of this command to disable the SNTP client.

This command enables the SNTP Broadcast and Anycast client on an interface. Use the `no` form of this command to disable the SNTP client.

**Syntax**

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

**Parameters**

N/A

**Default Configuration**

The SNTP client is disabled on an interface.

**Command Mode**

Interface Configuration (Ethernet, Port-channel, VLAN) mode

**User Guidelines**

The `sntp broadcast client enable` Global Configuration mode command globally enables Broadcast clients.

**Example**

The following example enables the SNTP Broadcast and Anycast client on an interface.

```text
switchxxxxxx(config-if)# sntp client enable
```
7.13 **sntp unicast client enable**

The `sntp unicast client enable` Global Configuration mode command enables the device to use Simple Network Time Protocol (SNTP)-predefined Unicast clients. Use the `no` form of this command to disable the SNTP Unicast clients.

**Syntax**

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

**Parameters**

N/A

**Default Configuration**

The SNTP unicast client is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the `sntp server` Global Configuration mode command to define SNTP servers.

**Example**

The following example enables the device to use SNTP Unicast clients.

```
switchxxxxxxx(config)# sntp unicast client enable
```

7.14 **sntp unicast client poll**

The `sntp unicast client poll` Global Configuration mode command enables polling for the SNTP predefined Unicast clients. Use the `no` form of this command to disable the polling for the SNTP client.

**Syntax**

```
sntp unicast client poll
no sntp unicast client poll
```

```
Default Configuration
Polling is disabled.

Command Mode
Global Configuration mode

Example
The following example enables polling for SNTP predefined unicast clients.

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

7.15 sntp server
The sntp server Global Configuration mode command configures the device to use the SNTP to request and accept Network Time Protocol (NTP) traffic from a specified server (meaning to accept system time from an SNTP server). Use the no form of this command to remove a server from the list of SNTP servers.

Syntax
```
sntp server {ip-address | hostname} [poll] [key keyid]
no sntp server {ip-address | hostname}
```

Parameters
- **ip-address**—Specifies the server IP address. This can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions:
- **hostname**—Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length for each part of the hostname: 63 characters)
- **poll**—Enables polling.
- **key keyid**—Specifies the Authentication key to use when sending packets to this peer. (Range: 1–4294967295)

Default Configuration
No servers are defined.
Command Mode
Global Configuration mode

User Guidelines
Up to 8 SNTP servers can be defined.
The `sntp unicast client enable` Global Configuration mode command enables predefined Unicast clients.
The `sntp unicast client poll` Global Configuration mode command globally enables polling.

Example
The following example configures the device to accept SNTP traffic from the server on 192.1.1.1 with polling.

```
switchxxxxxx(config)# sntp server 192.1.1.1 poll
```

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

Syntax
```
show clock [detail]
```

Parameters
detail—Displays the time zone and summer time configuration.

Command Mode
EXEC mode

Examples
Example 1 - The following example displays the system time and date.

```
switchxxxxxx# show clock
15:29:03 PDT(UTC-7) Jun 17 2002
```
Example 2 - The following example displays the system time and date along with the time zone and summer time configuration.

switchxxxxxx# show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP
Time zone:
Acronym is PST
Offset is UTC-8
Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
DHCP timezone: Disabled

7.17 show sntp configuration

The show sntp configuration Privileged EXEC mode command displays the SNTP configuration on the device.

Syntax

show sntp configuration

Parameters

N/A

Default Configuration

N/A
**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the device's current SNTP configuration.

```
switchxxxxxx# show sntp configuration
SNTP port : 123 .
Polling interval: 1024 seconds.
MD5 authentication keys
-----------------------------------
  2  John123
  3  Alice456
-----------------------------------
Authentication is not required for synchronization.
No trusted keys.

Unicast Clients: Enabled
Unicast Clients Polling: Enabled
Server       Polling   Encryption Key
------------- -------   --------------
 1.1.1.121    Disabled     Disabled

Broadcast Clients: disabled
Anycast Clients: disabled
No Broadcast Interfaces.
switchxxxxxx#
```

**7.18 show sntp status**

The `show sntp status` Privileged EXEC mode command displays the SNTP servers status.
**Syntax**

`show sntp status`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the SNTP servers status.

```
switchxxxxxx# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is afe2525e.70597b34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:

<table>
<thead>
<tr>
<th>Server</th>
<th>Status</th>
<th>Last response</th>
<th>Offset [mSec]</th>
<th>Delay [mSec]</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.1.1.8</td>
<td>Up</td>
<td>19:58:22.289 PDT Feb 19 2005</td>
<td>7.33</td>
<td>117.79</td>
</tr>
<tr>
<td>176.1.8.179</td>
<td>Unknown</td>
<td>12:17:17.987 PDT Feb 19 2005</td>
<td>8.98</td>
<td>189.19</td>
</tr>
</tbody>
</table>

Anycast server:

<table>
<thead>
<tr>
<th>Server</th>
<th>Interface</th>
<th>Status</th>
<th>Last response</th>
<th>Offset [mSec]</th>
<th>Delay [mSec]</th>
</tr>
</thead>
</table>
```
<table>
<thead>
<tr>
<th>Broadcast:</th>
<th>Interface</th>
<th>Last response</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.9.1.1</td>
<td>VLAN 119</td>
<td>19:17:59.792</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDT Feb 19 2002</td>
</tr>
</tbody>
</table>
DNS Client Commands

8.1 clear host

Use the **clear host** command in privileged EXEC mode to delete dynamic host-name-to-address mapping entries from the DNS client name-to-address cache.

Syntax

```
clear host {hostname /*}
```

Parameters

- **hostname**—Name of the host for which host-name-to-address mappings are to be deleted from the DNS client name-to-address cache.
- **/***—Specifies that all the dynamic host-name-to-address mappings are to be deleted from the DNS client name-to-address cache.

Default Configuration

No host-name-to-address mapping entries are deleted from the DNS client name-to-address cache.

Command Mode

Privileged EXEC mode

User Guidelines

To remove the dynamic entry that provides mapping information for a single hostname, use the *hostname* argument. To remove all dynamic entries, use the */* keyword.

To define a static host-name-to-address mappings in the DNS host name cache, use the *ip host* command.

To delete a static host-name-to-address mappings in the DNS host name cache, use the *no ip host* command.
Example

The following example deletes all dynamic entries from the DNS client name-to-address cache.

clear host *

82 ip domain lookup

Use the `ip domain lookup` command in Global Configuration mode to enable the IP Domain Naming System (DNS)-based host-name-to-address translation.

Use the `no` form of this command to disable the DNS.

Syntax

`ip domain lookup`

`no ip domain lookup`

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables DNS-based host-name-to-address translation.

```
switchxxxxxx(config)# ip domain lookup
```

83 ip domain name

Use the `ip domain name` command in Global Configuration mode to define a default domain name that the switch uses to complete unqualified host names (names without a dotted domain name).
Use the no form of this command to delete the static defined default domain name.

**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: 1–158 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 host name 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 host names 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 158 bytes.

**Example**

The following example defines the default domain name as ‘www.website.com’.

```
switchxxxxxx(config)# ip domain name website.com
```

**ip domain polling-interval**

Use the `ip domain polling-interval` command in Global Configuration mode to specify the polling interval.
Use the `no` form of this command to return to the default behavior.

**Syntax**

```
ip domain polling-interval seconds
no ip domain polling-interval
```

**Parameters**

- `seconds`—Polling interval in seconds. The range is from \((2 \times (R + 1) \times T)\) to 3600.

**Default Configuration**

The default value is \(2 \times (R + 1) \times T\), where

- \(R\) is a value configured by the `ip domain retry` command.
- \(T\) is a value configured by the `ip domain timeout` command.

**Command Mode**

Global Configuration mode

**User Guidelines**

Some applications communicate with the given IP address continuously. DNS clients for such applications, which have not received resolution of the IP address or have not detected a DNS server using a fixed number of retransmissions, return an error to the application and continue to send DNS Request messages for the IP address using the polling interval.

**Example**

The following example shows how to configure the polling interval of 100 seconds:

```
85 ip domain polling-interval 100
```

**ip domain retry**

Use the `ip domain retry` command in Global Configuration mode to specify the number of times the device will send Domain Name System (DNS) queries when there is no answer.

Use the `no` form of this command to return to the default behavior.
Syntax

`ip domain retry number`

`no ip domain retry`

Parameters

`number`—Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 16.

Default Configuration

The default value is 2.

Command Mode

Global Configuration mode

User Guidelines

The `number` argument specifies how many times the DNS query will be sent to a DNS server until the switch decides that the DNS server does not exist.

Example

The following example shows how to configure the device to send out 10 DNS queries before giving up:

```
ip domain retry 10
```

86  `ip domain timeout`

Use the `ip domain timeout` command in Global Configuration mode to specify the amount of time to wait for a response to a DNS query.

Use the `no` form of this command to return to the default behavior.

Syntax

`ip domain timeout seconds`

`no ip domain timeout`
Parameters

seconds—Time, in seconds, to wait for a response to a DNS query. The range is from 1 to 60.

Default Configuration

The default value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use the command to change the default time out value. Use the no form of this command to return to the default time out value.

Example

The following example shows how to configure the switch to wait 50 seconds for a response to a DNS query:

```
ip domain timeout  50
```

87 ip host

Use the ip host Global Configuration mode command to define the static host-name-to-address mapping in the DNS host name cache.

Use the no form of this command to remove the static-host name-to-address mapping.

Syntax

```
ip host  name address1 [address2...address8]
no ip host  name ip host  name [address1...address8]
```

Parameters

- name—Name of the host. Length: 1–158 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—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
Host names are restricted to ASCII letters A through Z (case-insensitive), the digits 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
The following example defines a static host-name-to-address mapping in the host cache.

```plaintext
ip host accounting.website.com 176.10.23.1
```

88  ip name-server

Use the ip name-server command in Global Configuration mode to specify the address of one or more name servers to use for name and address resolution.

Use the no form of this command to remove the static specified addresses.

Syntax
ip name-server server1-address [server-address2...server-address8]
no ip name-server [server-address1...server-address8]
Parameters

- server-address1—IPv4 or IPv6 addresses of a single name server.
- server-address2...server-address8—IPv4 or IPv6 addresses of additional name servers.

Default Configuration

No name server IP addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers is determined by the order in which they were entered.

Each `ip name-server` command replaces the configuration defined by the previous one (if one existed).

Example

The following example shows how to specify IPv4 hosts 172.16.1.111, 172.16.1.2, and IPv6 host 2001:0DB8::3 as the name servers:

```plaintext
ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

show hosts

Use the `show hosts` command in privileged EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

Syntax

`show hosts [all | hostname]`

Parameters

- all—The specified host name cache information is to be displayed for all configured DNS views. This is the default.
• **name**—The specified host name cache information displayed is to be limited to entries for a particular host name.

**Command Mode**

Privileged EXEC

**Default Configuration**

Default is all.

**User Guidelines**

This command displays the default domain name, a list of name server hosts, and the cached list of host names and addresses.

**Example**

The following is sample output of this command with no parameters specified:

```
show hosts
Name/address lookup is enabled
Domain Timeout: 3 seconds
Domain Retry: 2 times
Domain Polling Interval: 18 seconds
Default Domain Table

<table>
<thead>
<tr>
<th>Domain</th>
<th>Source</th>
<th>Interface</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>a222</td>
<td>static</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>grenl</td>
<td>DHCPv6</td>
<td>vlan 1</td>
<td>1</td>
</tr>
<tr>
<td>unit1</td>
<td>DHCPv6</td>
<td>vlan 1</td>
<td>2</td>
</tr>
<tr>
<td>expl1</td>
<td>DHCPv6</td>
<td>vlan 1</td>
<td>3</td>
</tr>
<tr>
<td>cisco.com</td>
<td>DHCPv4</td>
<td>gi2/1/24</td>
<td>1</td>
</tr>
</tbody>
</table>

Name Server Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Source</th>
<th>Interface</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.4.1</td>
<td>static</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
```
### DNS Client Commands

<table>
<thead>
<tr>
<th>Host</th>
<th>Addresses</th>
<th>Type</th>
<th>State</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1::1</td>
<td>DHCPv6 vlan 1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2::2</td>
<td>DHCPv6 vlan 1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3::3</td>
<td>DHCPv6 vlan 1</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.5.102.110</td>
<td>DHCPv4 gi2/1/24</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.5.102.111</td>
<td>DHCPv4 gi2/1/24</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Cache Table

Flags: (STA/DYN/FIX, OK/NE/??)

- STA - Static, DYN - Dynamic, FIX - Fixed
- OK - Okay, NE - Negative Cache, ?? - No Response

Remaining

<table>
<thead>
<tr>
<th>Host</th>
<th>Addresses</th>
<th>Type</th>
<th>State</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>173.194.34.96</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.101</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.104</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.110</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.103</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.105</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.97</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:14</td>
</tr>
<tr>
<td>google.com</td>
<td>173.194.34.99</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:01:06</td>
</tr>
<tr>
<td>pt-lt0109.a222</td>
<td>no resolution</td>
<td>IPv4</td>
<td>DYN,NE</td>
<td>0000:14:37</td>
</tr>
<tr>
<td>pt-lt0109.gren1</td>
<td>no resolution</td>
<td>IPv4</td>
<td>DYN,NE</td>
<td>0000:14:38</td>
</tr>
<tr>
<td>pt-lt0109.unit1</td>
<td>no resolution</td>
<td>IPv4</td>
<td>DYN,NE</td>
<td>0000:14:37</td>
</tr>
<tr>
<td>pt-lt0109.cisco.com</td>
<td>10.5.80.50</td>
<td>IPv4</td>
<td>DYN,OK</td>
<td>0000:19:37</td>
</tr>
</tbody>
</table>
9.1 **copy**

The *copy* Privileged EXEC mode command copies a source file to a destination file.

**Syntax**

```plaintext
copy source-url destination-url[exclude | include-encrypted | include-plaintext]
```

**Parameters**

- **source-url**—Specifies the source file URL or source file reserved keyword to be copied. (Length: 1–160 characters)

- **destination-url**—Specifies the destination file URL or destination file reserved keyword. (Length: 1–160 characters).

- **Flash://** —The source or destination URL scheme that specifies the access method to the local flash memory. It stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-config).

- **exclude**—Do not include sensitive data in the file being copied.

- **include-encrypted**—Include sensitive data in its encrypted form.

- **include-plaintext**—Include sensitive data in its plaintext form

The following table displays the URL options.

<table>
<thead>
<tr>
<th>Source and/or Destination URL</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>running-config</td>
<td>Currently running configuration file. This cannot be the destination file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Startup configuration file.</td>
</tr>
<tr>
<td>flash://startup-config</td>
<td></td>
</tr>
<tr>
<td>image</td>
<td>Image file. If specified as the source file, it is the active image file. If specified as the destination file, it is the non-active image file.</td>
</tr>
<tr>
<td>flash://image</td>
<td></td>
</tr>
<tr>
<td>Source and/or Destination URL</td>
<td>Source or Destination</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>boot</td>
<td>Boot file.</td>
</tr>
<tr>
<td>tftp://</td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is <code>tftp://host/[directory]/filename</code>. The host can be either an IP address or a host name.</td>
</tr>
<tr>
<td>scp://</td>
<td>Source or destination URL for a Secure Copy Protocol (SCP) network server. The syntax for this alias is: <code>scp://[username:password@]host/[directory]/filename</code>. The host can be either the IP address or hostname. The default on the switch is SSH authentication by password with username and password anonymous. The SSH authentication parameters can be reconfigured to match the SSH/SCP server’s parameters.</td>
</tr>
<tr>
<td>xmodem:</td>
<td>Source for the file from a serial connection that uses the Xmodem protocol.</td>
</tr>
<tr>
<td>null:</td>
<td>Null destination for copies or files. A remote file can be copied to null to determine its size. For instance <code>copy running-conf null</code> returns the size of the running configuration file.</td>
</tr>
<tr>
<td>backup-config</td>
<td>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-conf or startup-conf files.</td>
</tr>
<tr>
<td>mirror-config</td>
<td>Mirrored configuration file. If the running config and the startup config have been identical for 24 hours, the startup config is automatically copied to the mirror-conf file by the system. It can then be copied to the startup or running conf if required.</td>
</tr>
<tr>
<td>localization</td>
<td>This enables copying a language dictionary file to the secondary language file, such as in <code>copy tftp://10.5.234.203/french.txt localization</code>. This creates French as the second language. The file <code>french.txt</code> is the French dictionary.</td>
</tr>
</tbody>
</table>
Configuration and Image File Commands

Default Configuration

Sensitive data is excluded if no method was specified.

Command Mode

Privileged EXEC mode

User Guidelines

The location of the file system dictates the format of the source or destination URL.

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

IPv6z Address Format

If the IPv6 address is a Link Local address (IPv6z address), the outgoing interface name must be specified. The format of an IPv6z address is: 

{ipv6-link-local-address}%{interface-id}. The subparameters are:

- ipv6-link-local-address—Specifies the IPv6 Link Local address.
- interface-id—{<port-type>[ ]<port-number>|<port-channel | po>}[<port-channel-number> | {tunnel | tu}[<tunnel-number> | vlan[ ]<vlan-id>

If the egress interface is not specified, the default interface is selected. The following combinations are possible:

- ipv6_address%interface_id - Refers to the IPv6 address on the interface specified.
- ipv6_address%0 - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.
- ipv6_address - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

Invalid Combinations of Source and Destination

<table>
<thead>
<tr>
<th>Source and/or Destination URL</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit://member/localization</td>
<td>The secondary language file on one of the units. To copy to all units, specify * in the member field.</td>
</tr>
<tr>
<td>logging</td>
<td>Specifies the SYSLOG file.</td>
</tr>
<tr>
<td>Word&lt;1-128&gt;</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>
The following are invalid combinations of source and destination files:

- The source file and destination file are the same file.

- `xmodem:` is the destination file. The source file can be copied to `image`, `boot` and `null` only.

- `tftp://` is the source file and destination file on the same copy.

- `*.prv` files cannot be copied.

- The destination file cannot be the Running Configuration file.

- `mirror-config` cannot be used as a destination

The following table describes the characters displayed by the system when `copy` is being run:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).</td>
</tr>
<tr>
<td>.</td>
<td>For network transfers, indicates that the copy process timed out.</td>
</tr>
</tbody>
</table>

**Various Copy Options Guidelines**

- **Copying an Image File from a Server to Flash Memory**

  Use the `copy source-url flash://image` command to copy an image file from a server to flash memory. When the administrator copies an image file from the server to a device, the image file is saved to the "inactive" image. To use this image, the administrator must switch the inactive image to the active image and reboot. The device will then use this new image.

- **Copying a Boot File from a Server to Flash Memory**

  Use the `copy source-url boot` command to copy a boot file from a server to flash memory. Copying a Configuration File from a Server to the Startup Configuration

  Use the `copy source-url startup-config` command to copy a configuration file from a network server to the device startup configuration file. The startup configuration file is replaced by the copied configuration file.

- **Storing the Running Config or Startup Config on a Server**

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

### Saving the Running Configuration to the Startup Configuration

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

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

Use the `copy running-config backup-config` command to back up the running configuration to the backup configuration file.

Use the `copy startup-config backup-config` command to back up the startup configuration to the backup configuration file.

### Restoring the Mirror Configuration File.

Use `copy mirror-config startup-config` or `copy mirror-config running-config` to copy the mirror configuration file to one of the configuration files being used.

**SCP Copy Authentication Options**

The following options are possible for using the SCP copy feature:

- `scp://host/[directory]/filename`
  
  In this option, the SSH authentication method (either by password or by key) and the credentials are specified by the CLI commands for `ip ssh client (ip ssh-client authentication, ip ssh-client key-type or ip ssh-client password/username, and also the server authentication configuration commands),`

- `scp://username.password@host/[directory]/filename`
  
  This option specifies SSH authentication by password, and the user name and password for this specific SCP session (one-time only).

**Examples**
Example 1 - The following example copies system image file1 from the TFTP server 172.16.101.101 to the non-active image file.

```
switchxxxxxx# copy tftp://172.16.101.101/file1 image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Example 2 - Copying an Image from a Server to Flash Memory

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to a non-active image file.

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Example 3 - Copying the mirror-config file to the startup-configuration file

The following example copies the mirror configuration file, saved by the system, to the Startup Configuration file.

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

Example 4 - Copy file1 from SSH server to startup config
The following example copies file1 to the Startup Configuration file. The username and password used for SCP session authentication are: jeff and admin1. The IP address of the server containing file1 is 102.1.2.2.

```
switchxxxxxx# copy scp://jeff:admin1@102.1.2.2/file1 startup-config
```
9.2  write

Use the write Privileged EXEC mode command to save the running configuration to the startup configuration file.

Syntax

write [memory]

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following example shows how to overwrite the startup-config file with the running-config file with the write command.

```
switchxxxxxx# write
15-Sep-2010 11:27:50 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
```

9.3  delete

The delete Privileged EXEC mode command deletes a file from a flash memory device.

Syntax

delete url
Parameters

url—Specifies the location URL or reserved keyword of the file to be deleted. (Length: 1–160 characters)

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g., for copying the running configuration file, the user may either use flash://running-config or just running-config).

The following table displays keywords and URL prefixes:

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Startup configuration file.</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

mirror-config, *.sys, *.prv, image-1 and image-2 files cannot be deleted.

Example

The following example deletes the file called ‘backup-config’ from the flash memory.

```
switchxxxxxxx# delete flash://backup-config
Delete flash://backup-config? [confirm]
```

9.4 dir

The dir Privileged EXEC mode command displays the list of files on a flash file system.

Syntax

dir [directory-path]
Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the list of files on a flash file system

Total size of flash: 33292288 bytes
Free size of flash: 20708893 bytes

switchxxxxxx# dir

Directory of flash:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Permission</th>
<th>Flash Size</th>
<th>Data Size</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>backuplo</td>
<td>rw</td>
<td>851760</td>
<td>525565</td>
<td>22-Dec-2010 10:50:32</td>
</tr>
<tr>
<td>backup-config</td>
<td>rw</td>
<td>524288</td>
<td>104</td>
<td>01-Jan-2010 05:35:04</td>
</tr>
<tr>
<td>image-1</td>
<td>rw</td>
<td>10485760</td>
<td>10485760</td>
<td>01-Jan-2010 06:10:23</td>
</tr>
<tr>
<td>image-2</td>
<td>rw</td>
<td>10485760</td>
<td>10485760</td>
<td>01-Jan-2010 05:43:54</td>
</tr>
<tr>
<td>mirror-config</td>
<td>rw</td>
<td>524288</td>
<td>104</td>
<td>01-Jan-2010 05:35:04</td>
</tr>
<tr>
<td>dhcpsn.prv</td>
<td>--</td>
<td>262144</td>
<td>--</td>
<td>01-Jan-2010 05:25:07</td>
</tr>
<tr>
<td>syslog1.sys</td>
<td>r-</td>
<td>524288</td>
<td>--</td>
<td>01-Jan-2010 05:57:00</td>
</tr>
<tr>
<td>syslog2.sys</td>
<td>r-</td>
<td>524288</td>
<td>--</td>
<td>01-Jan-2010 05:57:00</td>
</tr>
<tr>
<td>directry.prv</td>
<td>--</td>
<td>262144</td>
<td>--</td>
<td>01-Jan-2010 05:25:07</td>
</tr>
<tr>
<td>startup-config</td>
<td>rw</td>
<td>786432</td>
<td>1081</td>
<td>01-Jan-2010 10:05:34</td>
</tr>
</tbody>
</table>

Total size of flash: 66322432 bytes
Free size of flash: 42205184 bytes
9.5 more

The `more` Privileged EXEC mode command displays a file.

Syntax

`more url`

Parameters

`url`—Specifies the location URL or reserved keyword of the source file to be displayed. (Length: 1–160 characters).

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-config).

The following table displays options for the URL parameter:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>running-config</td>
<td>Current running configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Startup configuration file.</td>
</tr>
<tr>
<td>mirror-config</td>
<td>Mirrored configuration file.</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Files are displayed in ASCII format, except for the images, which are displayed in a hexadecimal format.

*.prv files cannot be displayed.

Example

The following example displays the running configuration file contents.

```
switchxxxxxx# more running-config
```
no spanning-tree
interface range gi1-48
speed 1000
exit
no lldp run
line console
exec-timeout 0

9.6 boot system

The `boot system` Privileged EXEC mode command specifies the active system image file that will be loaded by the device at startup.

**Syntax**

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

**Parameters**

- **image-1**—Specifies that image-1 is loaded as the system image during the next device startup.
- **image-2**—Specifies that image-2 is loaded as the system image during the next device startup.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Use the `rename` command to display the active image.
Example
The following example specifies that image-1 is the active system image file loaded by the device at startup. The results of this command is displayed in rename.

```
switchxxxxx# boot system image-1
switchxxxxx# show bootvar
```

<table>
<thead>
<tr>
<th>Image</th>
<th>Filename</th>
<th>Version</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>image-1</td>
<td>1.1.0.73</td>
<td>19-Jun-2011 18:10:49</td>
<td>Not active*</td>
</tr>
<tr>
<td>2</td>
<td>image-2</td>
<td>1.1.0.73</td>
<td>19-Jun-2011 18:10:49</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

9.7 rename
The rename Privileged EXEC mode command renames a file.

Syntax
rename url new-url

Parameters
- url—Specifies the file location URL. (Length: 1–160 characters)
- new-url—Specifies the file’s new URL. (Length: 1–160 characters)

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g., for copying the running configuration file, the user may either use flash://running-config or just running-config).

The following table displays options for the URL parameter:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD&lt;1-12&gt;8&gt;</td>
<td>Name of file (e.g. backup-config).</td>
</tr>
</tbody>
</table>
Default Configuration
N/A

Command Mode
Privileged EXEC mode

User Guidelines
mirror-config, *.sys and *.prv files cannot be renamed.

Example
The following example renames the configuration backup file.

switchxxxxxx# rename backup-config m-config.bak

9.8 show bootvar

Use the show bootvar EXEC mode command to display the active system image file that was loaded by the device at startup, and to display the system image file that will be loaded after rebooting the switch.

Syntax
show bootvar

Parameters
N/A

Command Mode
EXEC mode
Example

The following example displays the active system image file that was loaded by the device at startup and the system image file that will be loaded after rebooting the switch.

```
switchxxxxxx# show bootvar
Image  filename  Version   Date             Status
-----  --------  -------    --------          -------
1      image-1  1.1.04    23-Jul-2010      Active
2      image-2  1.1.0.5   22-Jan-2010      Not active*
```

"*: Designates that the image was selected for the next boot.

9.9 show running-config

The `show running-config` Privileged EXEC mode command displays the entire current Running Configuration file contents or the contents of the file for the specified interface(s).

Syntax

```
show running-config [interface interface-id-list | detailed | brief]
```

Parameters

- `interface interface-id-list`—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.
- `detailed`—Displays configuration with SSL and SSH keys.
- `brief`—Displays configuration without SSL and SSH keys.

Default Configuration

All interfaces are displayed. If `detailed` or `brief` is not specified, the default is `detailed`.

Command Mode

Privileged EXEC mode
User Guidelines

The Running Configuration file does not contain all the information that can be displayed in the output. Only non-default configurations are displayed.

Examples

The following example displays the Running Configuration file contents.

**Example 1 - Show the entire Running Configuration file.**

```
switchxxxxx# show running-config
no spanning-tree
interface range gi1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxx#
```

**Example 2 - Show the entire Running Configuration file for ports 1 and 2.**

```
switchxxxxx# show running-config interface fastethernet1/1/1-2
interface fastethernet1/1/1
  back-pressure
duplex half
  spee 10
flowcontrol on
negotiation 10h 100h 100f
dot1x max-req 8
```
description "Hello World String"
lacp timeout short
lacp port-priority 1234
port security max 111
port security mode max-addresses
spanning-tree disable
spanning-tree portfast auto
spanning-tree link-type point-to-point
spanning-tree cost 200000
spanning-tree port-priority 224
spanning-tree guard root
spanning-tree mst 2 port-priority 64
spanning-tree mst 2 cost 2222
spanning-tree mst 4 port-priority 80
qos cos 6
traffic-shape 12345
switchport mode general
switchport general allowed vlan add 12,14-20 tagged
switchport general allowed vlan add 2-11,13,100,3000,3002,3004,3006,3008 untagged
switchport general map macs-group 1 vlan 111
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
interface fastethernet1/1/2
ip address 1.100.100.100 255.0.0.0
switchport mode trunk
switchport general map macs-group 1 vlan 111
switchport general map subnets-group 1 vlan 113
switchport general map protocols-group 1 vlan 112
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
switchport trunk native vlan 22

9.10  show startup-config

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

Syntax

show startup-config [interface interface-id-list]

Parameters

- interface interface-id-list—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.

Default Configuration

All interfaces are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

The Startup Configuration file does not contain all the information that can be displayed in the output. Only non-default configurations are displayed.

Examples

Example 1 - The following example displays the Startup Configuration file contents.

switchxxxxxx# show startup-config

no spanning-tree
interface range gi1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#

Example 2 - The following example displays the Startup Configuration file contents for ports 1 and 2.

switchxxxxxx# show startup-config interface gi1-2
interface gi1
  back-pressure
  duplex half
  speed 10
  flowcontrol on
  negotiation 10h 100h 100f
  dot1x max-req 8
  description "Hello World String"
  lACP timeout short
  lACP port-priority 1234
  port security max 111
  port security mode max-addresses
  spanning-tree disable
  spanning-tree portfast auto
  spanning-tree link-type point-to-point
  spanning-tree cost 200000
  spanning-tree port-priority 224
  spanning-tree guard root
  spanning-tree mST 2 port-priority 64
spanning-tree mst 2 cost 2222
spanning-tree mst 4 port-priority 80
qos cos 6
traffic-shape 12345
switchport mode general
switchport general allowed vlan add 12,14-20 tagged
switchport general allowed vlan add 2-11,13,100,3000,3002,3004,3006,3008 untagged
switchport general map macs-group 1 vlan 111
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
interface fastethernet1/1/2
ip address 1.100.100.100 255.0.0.0
switchport mode trunk
switchport general map macs-group 1 vlan 111
switchport general map subnets-group 1 vlan 113
switchport general map protocols-group 1 vlan 112
switchport general ingress-filtering disable
switchport general acceptable-frame-type untagged-only
switchport general pvid 111
switchport trunk native vlan 22

9.11 service mirror-configuration

Use the service mirror-configuration Global Configuration mode command to enable the mirror-configuration service. Use no service mirror-configuration command to disable the service.

Syntax

service mirror-configuration

no service mirror-configuration
Parameters
N/A

Default Configuration
The default configuration is mirror-configuration service enabled.

Command Mode
Global Configuration mode

User Guidelines
The mirror-configuration service automatically keeps a copy of the last known stable configuration (startup configuration that wasn't modified for 24H). The mirror-configuration file is not deleted when restoring to factory defaults.

When this service is disabled, the mirror-configuration file is not created and if such file already exists, it is deleted.

Note that enabling the service doesn't implicitly creates a mirror-configuration file.

Examples
Example 1: The following example disables the mirror-configuration service
no service mirror-configuration
This operation will delete the mirror-config file if exists. Do you want to continue? (Y/N) [N]

Example 2: The following example enables the mirror-configuration service
service mirror-configuration
Service is enabled.
Note that the running-configuration must be first copied to the startup-configuration in order to initiate backing up the startup-config to the mirror-config.

9.12 show mirror-configuration service
Use the show mirror-configuration service EXEC mode command to display the mirror-configuration service status.
Syntax

show mirror-configuration service

Command Mode

EXEC mode

Example

The following example displays the status of the mirror-configuration service

show mirror-configuration service

Mirror-configuration service is enabled
10.1 boot host auto-config

Use the **boot host auto-config** Global Configuration mode command to enable DHCP auto configuration via either the TFTP or SCP protocols. Use the no form of this command to disable DHCP auto configuration.

**Syntax**

```
boot host auto-config [tftp | scp | auto [extension]]
```

```
no boot host auto-config
```

**Parameters**

- **ftp**—Only the TFTP protocol is used by auto-configuration.
- **scp**—Only the SCP protocol is used by auto-configuration.
- **auto**—(Default) Auto-configuration uses the TFTP or SCP protocol depending on the configuration file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
  - **extension**—The SCP file extension. When no value is specified, 'scp' is used. (Range: 0–128)

**Default Configuration**

The auto option is the default.

**Command Mode**

Global Configuration mode

**Default Configuration**

Enabled by default.

**Examples**

**Example 1** - The following example specifies the auto mode and specifies "scon" as the SCP extension:

```
boot host auto-config auto scon
```
Example 2 - The following example specifies the auto mode and does not provide an SCP extension. In this case “scp” is used.

```
boot host auto-config auto
```

Example 3. The following example specifies that only the SCP protocol will be used:

```
boot host auto-config scp
```

10.2 show boot

Use the show boot Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

Syntax

```
show boot
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privilege EXEC mode

Examples

```
switchxxxxxx show boot
Auto Config
----------
Config Download via DHCP: enabled
Download Protocol Mode is SCP
SCP extension is scp
Next Boot Config Download via DHCP: default
```
10.3 ip dhcp tftp-server ip address

Use the `ip dhcp tftp-server ip address` Global Configuration mode command to set the TFTP or SCP server’s IP address. This address server as the default address used by a switch when it has not been received from the DHCP server.

Use the `no` form of this command to remove the address.

**Syntax**

```
ip dhcp tftp-server ip address ip-addr
no ip dhcp tftp-server ip address
```

**Parameters**

- `ip addr ip-addr`—Address of TFTP server

**Default Configuration**

No IP address

**Command Mode**

Global Configuration mode

**User Guidelines**

The backup server can be either a TFTP server or an SCP server.

**Examples**

```
switchxxxxxx(config)# ip dhcp tftp-server ip address 10.5.234.232
```

10.4 ip dhcp tftp-server file

Use the `ip dhcp tftp-server file` Global Configuration mode command to set the full file name of the configuration file to be downloaded on the TFTP or SCP server when it has not been received from the DHCP server. This serves as the default configuration file.

Use the `no` form of this command to remove the name.

**Syntax**

```
ip dhcp tftp-server file file-path
```

**Parameters**

- `file-path`—Full file name of the configuration file
no ip dhcp tftp-server file

Parameters

file-path—Full file path and name of the configuration file on TFTP server

Default Configuration

No file name

Command Mode

Global Configuration mode

User Guidelines

The path/file name, used in the download process, can be received from DHCP or this command as well.

Examples

```
switchxxxxxx(config)# ip dhcp tftp-server file conf/conf-file
```

**10.5 show ip dhcp tftp-server**

Use the `show ip dhcp tftp-server` EXEC mode command to display information about the TFTP server.

Syntax

```
show ip dhcp tftp-server
```

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC
Example

switchxxxxxx# show ip dhcp tftp server
tftp server address
server address
active 1.1.1.1 from sname
manual 2.2.2.2
file path on tftp server
file path on server
active conf/conf-file from option 67
11.1  management access-list

The `management access-list` Global Configuration mode command configures a management access list (ACL) and enters the Management Access-List Configuration command mode. Use the `no` form of this command to delete an ACL.

Syntax

```
management access-list name
no management access-list name
```

Parameters

- `name`—Specifies the ACL name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. This command enters the Management Access-List Configuration mode, where the denied or permitted access conditions are defined with the `deny` and `permit` commands.

If no match criteria are defined, the default value is `deny`.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the `management access-class` command to select the active access list.

The active management list cannot be updated or removed.

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.
Examples

Example 1 - The following example creates a management access list called mlist, configures management gi1 and gi9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit gi1
switchxxxxxx(config-macl)# permit gi9
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)# management access-class mlist
```

Example 2 - The following example creates a management access list called ‘mlist’, configures all interfaces to be management interfaces except gi1 and 9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny gi1
switchxxxxxx(config-macl)# deny gi9
switchxxxxxx(config-macl)# permit
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)# management access-class mlist
```

11.2 permit (Management)

The `permit` Management Access-List Configuration mode command sets permit rules (ACEs) for the management access list (ACL).

**Syntax**

```
permit [interface-id] [service service]
```

```
permit ip-source [ipv4-address | ipv6-address/ipv6-prefix-length] [mask [mask / prefix-length]] [interface-id] [service service]
```
Parameters

- **interface-id**:—Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service service** — Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address**— Specifies the source IPv4 address.
- **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.
- **mask mask** — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- **mask prefix-length** — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with Ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example permits all ports in the ACL called *mlist*

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit
```

11.3 **deny (Management)**

The **deny** Management Access-List Configuration mode command sets permit rules (ACEs) for the management access list (ACL).
Syntax

deny [interface-id] [service service]
deny ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service service**—Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address**—Specifies the source IPv4 address.
- **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.
- **mask mask**—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- **mask prefix-length**—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example denies all ports in the ACL called *mlist*.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny
```
11.4 management access-class

The management access-class Global Configuration mode command restricts management connections by defining the active management access list (ACL). To disable 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 device can be managed only from the console.
- **name**—Specifies the ACL name to be used. (Length: 1–32 characters)

Default Configuration

The default configuration is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an access list called mlist as the active management access list.

```bash
switchxxxxxx(config)# management access-class mlist
```

11.5 show management access-list

The show management access-list Privileged EXEC mode command displays management access lists (ACLs).

Syntax

show management access-list [name]
Parameters

name—Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

Default Configuration

All management ACLs are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the mlist management ACL.

```
switchxxxxxx# show management access-list mlist
-only
----------
deny
! (Note: all other access implicitly denied)
mlist
----
permit gi1
permit gi9
! (Note: all other access implicitly denied)
switchxxxxxx#
```

11.6 show management access-class

The `show management access-class` Privileged EXEC mode command displays information about the active management access list (ACLs).

Syntax

`show management access-class`
Command Mode
Privileged EXEC mode

Example
The following example displays the active management ACL information.

switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
Network Management Protocol (SNMP) Commands

12.1 snmp-server server

Use the `snmp-server server` Global Configuration mode command to enable the device to be configured by the SNMP protocol. Use the `no` form of this command to disable this function.

Syntax

```
snmp-server server
no snmp-server server
```

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server server
```

12.2 snmp-server community

Use the `snmp-server community` Global Configuration mode command to set the community access string (password) that permits access to SNMP commands (v1 and v2). This is used for SNMP commands, such as GETs and SETs.

This command configures both SNMP v1 and v2.

Use the `no` form of this command to remove the specified community string.
Syntax

snmp-server community community-string [ro | rw | su] [ip-address | ipv6-address] [mask mask | prefix prefix-length] [view view-name]

no snmp-server community community-string [ip-address]

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters). This string is used as an input parameter to `snmp-server user` for SNMP v3.
- **ro**—Specifies read-only access (default)
- **rw**—Specifies read-write access
- **su**—Specifies SNMP administrator access
- **view view-name**—Specifies the name of a view configured using the command `snmp-server view` (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for **su**, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables, are available. (Range: 1–30 characters)
- **ip-address**—Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet’s source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.

**Default Configuration**

No community is defined

**Command Mode**

Global Configuration mode
User Guidelines

The logical key of the command is the pair (community, ip-address). If ip-address is omitted then the key is (community, All-IPs). This means that there cannot be two commands with the same community, ip address pair.

The view-name 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 view-name (read-view and notify-view always, and for rw for write-view also).

Example

Defines a password for administrator access to the management station at IP address 1.1.1.121 and mask 255.0.0.0.

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

12.3 snmp-server community-group

Use `snmp-server community-group` to configure access rights to a user group. The group must exist in order to be able to specify the access rights. This command configures both SNMP v1 and v2.

Syntax

```
snmp-server community-group community-string group-name [ip-address | ipv6-address] [mask mask | prefix prefix-length]
```

Parameters

- `community-string`—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters). This string is used as an input parameter to `snmp-server user` for SNMP v3.

- `ip-address`—Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
Network Management Protocol (SNMP) Commands

- **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.

- **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.

- **group-name**—This is the name of a group configured using `snmp-server group` with v1 or v2 (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)

**Default Configuration**

No community is defined

**Command Mode**

Global Configuration mode

**User Guidelines**

The **group-name** 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**

Defines a password **tom** for the group **abcd** that enables this group to access the management station 1.1.1.121 with prefix 8.

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

**12.4 snmp-server view**

The **snmp-server view** Global Configuration mode command creates or updates an SNMP view. Use the no form of this command to remove an SNMP view.
Syntax

`snmp-server view view-name oid-tree {included | excluded}`

`no snmp-server view view-name [oid-tree]`

Parameters

- **view-name**—Specifies the name for the view that is being created or updated. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System and, optionally, a sequence of numbers. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. This parameter depends on the MIB being specified.
- **included**—Specifies that the view type is included.
- **excluded**—Specifies that the view type is excluded.

Default Configuration

The following views are created by default:

- **Default** - Contains all MIBs except for those that configure the SNMP parameters themselves.
- **DefaultSuper** - Contains all MIBs.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view.

The command’s logical key is the pair (view-name, oid-tree). Therefore there cannot be two commands with the same view-name and oid-tree.

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.
Example
The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group (this format is specified on the parameters specified in ifEntry).

```
switchxxxxxxx(config)# snmp-server view user-view system included
switchxxxxxxx(config)# snmp-server view user-view system.7 excluded
switchxxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

12.5 show snmp views
Use the show snmp views Privileged EXEC mode command to display the SNMP views.

Syntax
```
show snmp views [viewname]
```

Parameters
viewname—Specifies the view name. (Length: 1–30 characters)

Default Configuration
If viewname is not specified, all views are displayed.

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP views.

```
switchxxxxxxx# show snmp views

<table>
<thead>
<tr>
<th>Name</th>
<th>OID Tree</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>iso</td>
<td>Included</td>
</tr>
<tr>
<td>Default</td>
<td>snmpNotificationMIB</td>
<td>Excluded</td>
</tr>
<tr>
<td>DefaultSuper</td>
<td>iso</td>
<td>Included</td>
</tr>
</tbody>
</table>
```
12.6 snmp-server group

Use the snmp-server group Global Configuration mode command to configure an SNMP group. Groups are used to map SNMP users to SNMP views (using snmp-server user). Use the no form of this command to remove an SNMP group.

Syntax

```
snmp-server group groupname {v1 | v2 | v3 [noauth | auth | priv] [notify notifyview]} [read readview] [write writeview]
```

```
no snmp-server group groupname {v1 | v2 | v3 [noauth | auth | priv]}
```

Parameters

- **group groupname**—Specifies the group name. (Length: 1–30 characters)
- **v1**—Specifies the SNMP Version 1 security model.
- **v2**—Specifies the SNMP Version 2 security model.
- **v3**—Specifies the SNMP Version 3 security model.
- **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.
- **notify notifyview**—Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgement. Applicable only to the SNMP version 3 security model. (Length: 1–30 characters)
- **read readview**—Specifies the view name that enables viewing only. (Length: 1–30 characters)
- **write writeview**—Specifies the view name that enables configuring the agent. (Length: 1–30 characters)

Default Configuration

No group entry exists.
If `notifyview` is not specified, the notify view is not defined.

If `readview` is not specified, all objects except for the community-table and SNMPv3 user and access tables are available for retrieval.

If `writeview` 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 `snmp-server user` to map users to the group. These users are then automatically mapped to the views defined in this command.

The command logical key is `(groupname, snmp-version, security-level)`. For `snmp-version v1/v2` the security-level is always `noauth`.

**Example**

The following example attaches a group called `user-group` to SNMPv3, assigns the encrypted security level to the group, and limits the access rights of a view called `user-view` to read-only. User `tom` is then assigned to `user-group`. So that user `tom` has the rights assigned in `user-view`.

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read user-view
switchxxxxxx(config)# snmp-server user tom user-group v3
```

### 12.7 `show snmp groups`

Use the `show snmp groups` Privileged EXEC mode command to display the configured SNMP groups.

**Syntax**

```
show snmp groups [groupname]
```

**Parameters**

`groupname`—Specifies the group name. (Length: 1–30 characters)
Default Configuration
Display all groups.

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP groups.

```
switchxxxxxx# show snmp groups
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Security</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Model</td>
<td>Read</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>user-group</td>
<td>V3</td>
<td>Default</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3</td>
<td>Default</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown above.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Group name.</td>
</tr>
<tr>
<td>Security</td>
<td>Model (SNMP model in use (v1, v2 or v3)).</td>
</tr>
<tr>
<td>Security</td>
<td>Level (Packet authentication with encryption. Applicable to SNMP v3 security only).</td>
</tr>
<tr>
<td>Views</td>
<td>Read (View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available).</td>
</tr>
<tr>
<td></td>
<td>Write (View name enabling data entry and managing the agent contents).</td>
</tr>
<tr>
<td></td>
<td>Notify (View name enabling specifying an inform or a trap).</td>
</tr>
</tbody>
</table>

12.8 snmp-server user
Use the `snmp-server user` Global Configuration mode command to configure a new SNMP Version user. Use the `no` form of the command to remove a user. Use the encrypted form of this command to enter the authentication and privacy passwords in encrypted form (see SSD).
Syntax

```plaintext
snmp-server user username groupname [v1 / v2c / [remote host] v3[auth { md5 / sha} auth-password [priv priv-password]]]
```

```plaintext
encrypted snmp-server user username groupname [v1 / v2c / [remote host] v3[auth { md5 / sha} encrypted-auth-password [priv encrypted-priv-password]]]
```

```plaintext
no snmp-server user username [remote host]
```

Parameters

- **username**—Define the name of the user on the host that connects to the agent. (Range: Up to 20 characters). For SNMP v1 or v2c, this username must match the community string entered in `snmp-server host`.

- **groupname**—The name of the group to which the user belongs. The group should be configured using the command `snmp-server group` with v1 or v2c parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)

- **remote host**—IP address (IPv4, IPv6 or IPv6z) or host name of the remote SNMP host. See IPv6z Address Conventions.

- **v1**—Specifies that the user is a v1 user.

- **v2c**—Specifies that the user is a v2c user.

- **v3**—Specifies that the user is a v3 user.

- **auth**—Specifies which authentication level is to be used.

- **md5**—Specifies the HMAC-MD5-96 authentication level.

- **Sha**—Specifies the HMAC-SHA-96 authentication level.

- **auth-password**—Specifies the authentication password. Range: Up to 32 characters.

- **encrypted-auth-password**—Specifies the authentication password in encrypted format.

- **priv-password**—Specifies the privacy password (The encryption algorithm used is data encryption standard - DES). Range: Up to 64 characters. **encrypted-priv-password**—Specifies the privacy password in encrypted format.
Default Configuration
No group entry exists.

Command Mode
Global configuration

User Guidelines
For SNMP v1 and v2, this performs the same actions as `snmp-server community-group`, except that `snmp-server community-group` configures both v1 and v2 at the same time. With this command, you must perform it once for v1 and once for v2.

When you enter a `show running-config` command, you do not see a line for this SNMP user. To see if this user has been added to the configuration, type the `show snmp user` command.

An SNMP EngineID must be defined in order to add SNMPv3 users to the device (in the `snmp-server engineID local` or `snmp-server engineID remote` commands).

Changing or removing the value of `snmpEngineID` deletes the SNMPv3 users' database.

The logical key of the command is `username`.

Configuring a remote host is required in order to send informs to that host, because an inform is a trap that requires acknowledgement. A configured remote host is also able to manage the device (besides getting the informs).

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID remote` command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

Since the same group may be defined several times, each time with different version or different access level (noauth, auth or auth & priv), when defining a user it is not sufficient to specify the group name, rather you must specify group name, version and access level for complete determination of how to handle packets from this user.
Example
This example assigns user *tom* to group *abcd* using SNMP v1 and v2c. The default is assigned as the engineID. User *tom* is assigned to group *abcd* using SNMP v1 and v2c.

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user tom acbd v3
```

### 12.9 show snmp users
Use the `show snmp users` Privileged EXEC mode command to display the configured SNMP users.

**Syntax**
```
show snmp users [username]
```

**Parameters**
- `username`—Specifies the user name. (Length: 1–30 characters)

**Default Configuration**
Display all users.

**Command Mode**
Privileged EXEC mode

**Example**
The following example displays the configured SNMP users

```
Example
The following example displays the configured SNMP users
```

```
console#show snmp users
User name : u1rem
  Group name : group1
  Authentication Algorithm : None
```
Privacy Algorithm : None
Remote : 11223344556677
Auth Password :
Priv Password :

User name : qqq
Group name : www
Authentication Algorithm : MD5
Privacy Algorithm : None
Remote :
Auth Password : helloworld1234567890987665
Priv Password :

User name : hello
Group name : world
Authentication Algorithm : MD5
Privacy Algorithm : DES
Remote :
Auth Password (encrypted):
Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLrAgOE6XQKTCqMIrnpWuHraRIZj
Priv Password (encrypted):
kN1ZHsSLo6WxIkuZVzhLOo1gl5waaNf7Vq6yLBpJdS4N68tL1tbTRSz2H4c4Q4
User name : u1noAuth
Group name : group1
Authentication Algorithm : None
Privacy Algorithm : None
Remote :
Auth Password (encrypted):
Priv Password (encrypted):
User name : u1OnlyAuth
Group name : group1
Authentication Algorithm : SHA
Privacy Algorithm : None
Remote :
Auth Password (encrypted):
8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
Priv Password (encrypted):

12.10 snmp-server filter

The snmp-server filter Global Configuration mode command creates or updates an SNMP server notification filter. Use the no form of this command to remove a notification filter.

Syntax

snmp-server filter filter-name oid-tree {included | excluded}
no snmp-server filter filter-name [oid-tree]

Parameters

- **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the filter in other commands. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Specifies that the filter type is included.
- **excluded**—Specifies that the filter type is excluded.
Default Configuration
No view entry exists.

Command Mode
Global Configuration mode

User Guidelines
This command can be entered multiple times for the same filter. If an object identifier is included in two or more lines, later lines take precedence. The command's logical key is the pair (filter-name, oid-tree).

Example
The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group (this format depends on the parameters define din ifEntry).

```
switchxxxxxx(config)# snmp-server filter f1 system included
switchxxxxxx(config)# snmp-server filter f2 system.7 excluded
switchxxxxxx(config)# snmp-server filter f3 ifEntry.*.1 included
```

12.11 show snmp filters
Use the show snmp filters Privileged EXEC mode command to display the defined SNMP filters.

Syntax
```
show snmp filters [filtername]
```

Parameters

filtername—Specifies the filter name. (Length: 1–30 characters)

Default Configuration
If filtername is not defined, all filters are displayed.

Command Mode
Privileged EXEC mode
Example

The following example displays the configured SNMP filters.

```
switchxxxxxx# show snmp filters user-filter
Name    OID Tree       Type
---------- ----------------- -----
user-filter  1.3.6.1.2.1.1     Included
user-filter  1.3.6.1.2.1.1.7   Excluded
user-filter  1.3.6.1.2.1.2.2.1.*.1 Included
```

12.12 snmp-server host

Use the `snmp-server host` Global Configuration mode command to configure the host for SNMP notifications: (traps/informs). Use the `no` form of this command to remove the specified host.

Syntax

```
snmp-server host [host-ip / hostname] [traps / informs] [version {1 | 2c | 3 [auth / noauth / priv]}] [community-string] [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

```
no snmp-server host [ip-address / hostname] [traps / informs] [version {1 | 2c | 3}]
```

Parameters

- **host-ip**—IP address of the host (the targeted recipient). The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **hostname**—Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- **trap**—Sends SNMP traps to this host (default).
- **informs**—Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.
- **1**—SNMPv1 traps are used.
- **2c**—SNMPv2 traps or informs are used
- **3**—SNMPv2 traps or informs are used
- **community-string**—Password-like community string sent with the notification operation. (Range: 1–20 characters). For v1 and v2, any community string can be entered here. For v3, the community string must match the user name defined in `snmp-server user` for v3.

- Authentication options are available for SNMP v3 only. The following options are available:
  - `noauth`—Specifies no authentication of a packet.
  - `auth`—Specifies authentication of a packet without encryption.
  - `priv`—Specifies authentication of a packet with encryption.

- **udp-port port**—UDP port of the host to use. The default is 162. (Range: 1–65535)

- **filter filtername**—Filter for this host. If unspecified, nothing is filtered. The filter is defined using `snmp-server filter` (no specific order of commands is imposed on the user). (Range: Up to 30 characters)

- **timeout seconds**—(For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)

- **retries retries**—(For informs only) Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. (Range: 0–255)

**Default Configuration**

Version: SNMP V1  
Type of notification: Traps  
udp-port: 162  
If informs are specified, the default for retries: 3  
Timeout: 15

**Command Mode**

Global Configuration mode

**User Guidelines**

The logical key of the command is the list - ip-address/hostname, traps/informs, version.
When configuring SNMP v1 or v2 notifications recipient, the software automatically generates a notification view for that recipient for all MIBs.

For SNMPv3 the software does not automatically create a user or a notify view.

Use the commands `snmp-server user` and `snmp-server group` to create a user or a group.

**Example**
The following defines a host at the IP address displayed.

```bash
switchxxxxxx(config)# snmp-server host 1.1.1.121 abc
```

### 12.13 snmp-server engineID remote

To specify the SNMP engine ID of a remote SNMP device, use the `snmp-server engineID remote` Global Configuration mode command. Use the `no` form of this command to remove the configured engine ID.

**Syntax**

```
snmp-server engineID remote [ip-address] engineid-string

no snmp-server engineID remote [ip-address]
```

**Parameters**

- `ip-address` — IPv4, IPv6 or IPv6z address of the remote device. See IPv6z Address Conventions.

- `engineid-string` — The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. If the user enters an odd number of hexadecimal digits, the system automatically prefixes the hexadecimal string with a zero. (Range: engineid-string 5–32 characters, 9–64 hexadecimal digits)

**Default Configuration**
The remote engineID is not configured by default.

**Command Mode**
Global Configuration mode
User Guidelines

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

12.14 snmp-server engineID local

The `snmp-server engineID local` Global Configuration mode command specifies the SNMP engineID on the local device for SNMP v3. Use the `no` form of this command to remove this engine ID.

Syntax

```
snmp-server engineID local {engineid-string | default}
no snmp-server engineID local
```

Parameters

- `engineid-string`—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)

- `default`—Specifies that the engine ID is created automatically based on the device MAC address.

Default Configuration

The default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

Command Mode

Global Configuration mode
User Guidelines

To use SNMPv3, an engine ID must be specified for the device. Any ID can be specified or the default string, which is generated using the device MAC address, can be used.

Since the engineID should be unique within an administrative domain, use the default keyword to configure the Engine ID.

Changing or removing the value of `snmpEngineID` deletes the SNMPv3 users database.

The SNMP EngineID cannot be all 0x0 or all 0xF or 0x00000001

Example

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
switchxxxxxx(config)# snmp-server engineid local default
```

The engine-id must be unique within your administrative domain.

Do you wish to continue? [Y/N] Y

The SNMPv3 database will be erased. Do you wish to continue? [Y/N] Y

12.15 show snmp engineID

Use the `show snmp engineID` Privileged EXEC mode command to display the local SNMP engine ID.

Syntax

```
show snmp engineID
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode
Example

The following example displays the SNMP engine ID.

```
switchxxxxxx # show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
IP address  Remote SNMP engineID
----------- -------------------------------
172.16.1.1  08009009020C0B099C075879
```

12.16  snmp-server enable traps

Use the `snmp-server enable traps` Global Configuration mode command to enable the device to send all SNMP traps. Use the `no` form of the command to disable all SNMP traps.

Syntax

```
snmp-server enable traps
no snmp-server enable traps
```

Default Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

If `no snmp-server enable traps` has been entered, you can enable failure traps by using `snmp-server trap authentication` as shown in the example.

Example

The following example enables SNMP traps except for SNMP failure traps.

```
switchxxxxxx(config)# snmp-server enable traps
switchxxxxxx(config)# no snmp-server trap authentication
```
### 12.17 snmp-server trap authentication

Use the `snmp-server trap authentication` Global Configuration mode command to enable the device to send SNMP traps when authentication fails. Use the `no` form of this command to disable SNMP failed authentication traps.

**Syntax**

```plaintext
snmp-server trap authentication
no snmp-server trap authentication
```

**Parameters**

N/A

**Default Configuration**

SNMP failed authentication traps are enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

The command `snmp-server enable traps` enables all traps including failure traps. Therefore, if that command is enabled (it is enabled by default), this command is not necessary.

**Example**

The following example disables all SNMP traps and enables only failed authentication traps.

```plaintext
switchxxxxxx(config)# no snmp-server enable traps
switchxxxxxx(config)# snmp-server trap authentication
```

### 12.18 snmp-server contact

Use the `snmp-server contact` Global Configuration mode command to set the value of the system contact (sysContact) string. Use the `no` form of the command to remove the system contact information.
Network Management Protocol (SNMP) Commands

12.18 snmp-server contact

Syntax

```
snmp-server contact text
no snmp-server contact
```

Parameters

text—Specifies system contact information. (Length: 1–168 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

The following example sets the system contact information to Technical_Support.

```
switchxxxxxx(config)# snmp-server contact Technical_Support
```

12.19 snmp-server location

Use the `snmp-server location` Global Configuration mode command to set the value of the system location string. Use the `no` form of this command to remove the location string.

Syntax

```
snmp-server location text
no snmp-server location
```

Parameters

text—Specifies the system location information. (Length: 1–160 characters)

Default Configuration

N/A
Command Mode
Global Configuration mode

Example
The following example sets the device location to New_York.

```
switchxxxxxx(config)# snmp-server location New_York
```

12.20 snmp-server set

Use the `snmp-server set` Global Configuration mode command to define SNMP MIB commands in the configuration file if a MIB performs an action for which there is no corresponding CLI command.

Syntax
```
snmp-server set variable-name name value [name2 value2..]
```

Parameters
- **variable-name**—Specifies an SNMP MIB variable name, which must be a valid string.
- **name value**—Specifies a list of names and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

Default Configuration
N/A

Command Mode
Global Configuration mode

User Guidelines
Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent CLI command. To generate configuration files that support those situations, the system uses `snmp-server set`. This command is not intended for the end user.
Example

The following example configures the scalar MIB sysName with the value TechSupp.

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```
Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Community</th>
<th>Version</th>
<th>UDP Port</th>
<th>Filter Name</th>
<th>TO Sec</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.122.173.42</td>
<td>Trap</td>
<td>public</td>
<td>2</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>192.122.173.42</td>
<td>Inform</td>
<td>public</td>
<td>2</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>

Version 3 notifications

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Username</th>
<th>Security Level</th>
<th>UDP Port</th>
<th>Filter name</th>
<th>TO Sec</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.122.173.42</td>
<td>Inform</td>
<td>Bob</td>
<td>Priv</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>

System Contact: Robert
System Location: Marketing

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community-string</td>
<td>The community access string permitting access to SNMP.</td>
</tr>
<tr>
<td>Community-access</td>
<td>The permitted access type—read-only, read-write, super access.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The management station IP Address.</td>
</tr>
<tr>
<td>Target Address</td>
<td>The IP address of the targeted recipient.</td>
</tr>
<tr>
<td>Version</td>
<td>The SNMP version for the sent trap.</td>
</tr>
</tbody>
</table>
13.1 ip http server

Use the ip http server Global Configuration mode command to enable configuring and monitoring the device from a web browser. Use the no form of this command to disable this function.

Syntax

ip http server

no ip http server

Parameters

N/A

Default Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

Example

The following example enables configuring the device from a web browser.

switchxxxxxx(config)# ip http server

13.2 ip http port

The ip http port Global Configuration mode command specifies the TCP port used by the web browser interface. Use the no form of this command to restore the default configuration.

Syntax

ip http port port-number
no ip http port

Parameters

port port-number—For use by the HTTP server. (Range: 0–65534)

Default Configuration

The default port number is 80.

Command Mode

Global Configuration mode

Example

The following example configures the http port number as 100.

```
switchxxxxxx(config)# ip http port 100
```

13.3  ip http timeout-policy

Use the ip http timeout-policy Global Configuration mode command to set the interval for the system to wait for user input in http/https sessions before automatic logoff. Use the no form of this command to return to the default value.

Syntax

ip http timeout-policy idle-seconds [http-only | https-only]

no ip http timeout-policy

Parameters

idle-seconds—Specifies the maximum number of seconds that a connection is kept open if no data is received or response data cannot be sent out. (Range: 0–86400)

http-only —The timeout is specified only for http

https-only— The timeout is specified only for https

Default Configuration

600 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 be 1000 seconds.

```
switchxxxxxx(config)# ip http timeout-policy 1000
```

## 13.4 ip http secure-server

Use the **ip http secure-server** Global Configuration mode command to enable the device to be configured or monitored securely from a browser. Use the no form of this command to disable this function.

**Syntax**

```
ip http secure-server
no ip http secure-server
```

**Parameters**

N/A

**Default Configuration**

Disabled

**Command Mode**

Global Configuration mode

**User Guidelines**

After this command is used, you must generate a certificate using **crypto certificate generate**. If no certificate is generated, this command has no effect.

**Example**
13.5  **ip https certificate**

Use the **ip https certificate** Global Configuration mode command to configure the active certificate for HTTPS. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
ip https certificate number
```

```
no ip https certificate
```

**Parameters**

- **number**—Specifies the certificate number. (Range: 1–2)

**Default Configuration**

The default certificate number is 1.

**Command Mode**

Global Configuration mode

**User Guidelines**

First, use **crypto certificate generate** to generate one or two HTTPS certificates. Then use this command to specify which is the active certificate.

**Example**

The following example configures the active certificate for HTTPS.

```
switchxxxxxx(config)# ip https certificate 2
```

13.6  **show ip http**

The **show ip http** EXEC mode command displays the HTTP server configuration.
**Web Server Commands**

**Syntax**

`show ip http`

**Command Mode**

EXEC mode

**Example**

The following example displays the HTTP server configuration.

```
switchxxxxxx# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes
```

**13.7 show ip https**

The `show ip https` Privileged EXEC mode command displays the HTTPS server configuration.

**Syntax**

`show ip https`

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the HTTPS server configuration.

```
switchxxxxxx# show ip https
HTTPS server enabled
Port: 443
Interactive timeout: Follows the HTTP interactive timeout (10 minutes)
Certificate 1 is active
Issued by: www.verisign.com
```
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
14.1 ip telnet server

Use the ip telnet server Global Configuration mode command to enable the device as a Telnet server that accepts connection requests from remote Telnet clients. Remote Telnet clients can configure the device through the Telnet connections.

Use the no form of this command to disable the Telnet server functionality on the device.

Syntax

ip telnet server
no ip telnet server

Default Configuration

The Telnet server functionality on the device is disabled by default

Command Mode

Global Configuration mode

User Guidelines

The device can be enabled to accept connection requests from both remote SSH and Telnet clients. It is recommended that the remote client connects to the device using SSH (as opposed to Telnet), since SSH is a secure protocol and Telnet is not. To enable the device to be a SSH server, use the ip ssh server Global Configuration mode command

Example

The following example enables the device to be configured from a Telnet server.

switchxxxxxx(config)# ip telnet server
14.2 ip ssh server

The `ip ssh server` Global Configuration mode command enables the device to be an SSH server and so to accept connection requests from remote SSH clients. Remote SSH clients can manage the device through the SSH connection.

Use the `no` form of this command to disable the SSH server functionality from the device.

**Syntax**

```
ip ssh server
no ip ssh server
```

**Default Configuration**

The SSH server functionality is disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

The device as a SSH server generates the encryption keys automatically.

To generate new SSH server keys, use the `crypto key generate dsa` and `crypto key generate rsa` Global Configuration mode commands.

**Example**

The following example enables configuring the device to be an SSH server.

```
switchxxxxxx(config)# ip ssh server
```

14.3 ip ssh port

The `ip ssh port` Global Configuration mode command specifies the port used by the SSH server. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
ip ssh port port-number
```
no ip ssh port

Parameters

port-number—Specifies the port number to be used by the SSH server. (Range: 1–65535)

Default Configuration

The default port number is 22.

Command Mode

Global Configuration mode

Example

The following example specifies that port number 8080 is used by the SSH server.

```
switchxxxxxx(config)# ip ssh port 8080
```

14.4 ip ssh pubkey-auth

Use the `ip ssh pubkey-auth` Global Configuration mode command to enable public key authentication of incoming SSH sessions.

Use the `no` form of this command to disable this function.

Syntax

```
ip ssh pubkey-auth [auto-login]
no ip ssh pubkey-auth
```

Parameters

auto-login—Specifies that the device management AAA authentication is not needed. By default, this login is required after the SSH authentication.

Default Configuration

Public key authentication of incoming SSH sessions is disabled.

Auto-login is not enabled.
Command Mode
Global Configuration mode

User Guidelines
This command enables public key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for selecting one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device, except if the auto-login parameter was specified.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

The auto-login keyword works as follows:

- **Specified**—Management access is granted if SSH authentication succeeds and the name of SSH used is found in the local user database. The device management AAA authentication is transparent to the user. If the user name is not in the local user database, the user receives a warning message, and the user must pass the device management AAA authentication independently of the SSH authentication.

- **Not Specified**—Management access is granted only if the user passes both SSH authentication and device management AAA authentication independently. If no SSH authentication method is enabled, management access is granted only if the user is AAA-authenticated by the device management. No SSH authentication method means SSH is enabled, but neither SSH authentication by public key nor password is enabled.

Example
The following example enables authentication of the SSH client with no double authentication.

```
switchxxxxxx(config)# ip ssh pubkey-auth auto-login
```

14.5 ip ssh password-auth
Use the ip ssh password-auth Global Configuration mode command to enable password authentication of incoming SSH sessions.
Use the `no` form of this command to disable this function.

**Syntax**

```
ip ssh password-auth
no ip ssh password-auth
```

**Default Configuration**

Password authentication of incoming SSH sessions is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables password authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all locally-enabled SSH authentication methods and a remote SSH client must select one of them.

If the password method was chosen by the client, management access is granted after the client is authenticated by SSH using the regular user authentication (AAA). No login is needed from the device management.

If no SSH authentication method is enabled, management access is granted only if the user is authenticated by the device management (through AAA). If no SSH authentication method is selected, SSH is enabled, but neither SSH authentication by public key nor password is enabled.

**Example**

The following example enables password authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh password-auth
```

### 14.6 crypto key pubkey-chain ssh

The `crypto key pubkey-chain ssh` Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify device public keys, such as SSH client public keys.
Syntax

crypto key pubkey-chain ssh

Default Configuration

Keys do not exist.

Command Mode

Global Configuration mode

User Guidelines

Use this command when you want to manually specify SSH client’s public keys.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to the user ‘bob’.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string
AAAAB3NzaClyc2EAAAAADAQABAAAAAQAQCvTnRwPWL
Al4kpqiw9GBRonZQZxjHKcqKl6rM1Q+
ZNxfZSkvHG+QusIZ/76IlmFT34v7u7ChFAE+
Vu4GRfpSwoQuV35LqJJk67IOU/zfwO11g
kTwm175QR9hujS6WGNZQMXgh3ub8gDjTSq
muSn/Wd05iDXZ1ExQUw08licglk02LYciz
+Z4TrEU/9FJxwPlVQOjc+KBXuR0juNg5nFYsY
0Zck0N/W9a/tnkmlshRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfcej166DqVX1gWmN
zNR4DYDvSzg0DnwC4C8Qh
```
14.7 user-key

The **user-key** SSH Public Key-string Configuration mode command associates a username with a manually-configured SSH public key.

Use the **no user-key** command to remove an SSH user and the associated public key.

**Syntax**

```
user-key username {rsa | dsa}
no user-key username
```

**Parameters**

- **username**—Specifies the remote SSH client username. (Length: 1–48 characters)
- **rsa**—Specifies that the RSA key pair is manually configured.
- **dsa**—Specifies that the DSA key pair is manually configured.

**Default Configuration**

No SSH public keys exist.

**Command Mode**

SSH Public Key-string Configuration mode

**User Guidelines**

After entering this command, the existing key, if any, associated with the user will be deleted. You must follow this command with the **key-string** command to configure the key to the user.

**Example**

The following example enables manually configuring an SSH public key for SSH public key-chain `bob`.

```plaintext
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string row
```
14.8 key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

**Syntax**

`key-string [row key-string]`

**Parameters**

- **row**—Specifies the SSH public key row by row. The maximum length of a row is 160 characters.
- **key-string**—Specifies the key in UU-encoded DER format. UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

**Default Configuration**

Keys do not exist.

**Command Mode**

SSH Public Key-string Configuration mode

**User Guidelines**

Use the **key-string** SSH Public Key-string Configuration mode command without the **row** parameter to specify which SSH public key is to be interactively configured next. Enter a row with no characters to complete the command.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a **key-string row** command.

The UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

**Example**

The following example enters public key strings for SSH public key client ‘bob’.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
```
Telnet, Secure Shell (SSH) and Secure Login (Slogin) Commands

switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWlA14kpqIw9GBRonZQQZxjHKcqKL6rM1Q+
ZNxfZSkvHG+QusIZ/76IImFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJj67IOU/zfwO1lg
kTwm175QR9gHujS6KwGNQWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz+
+Z4TrEU/9FJxwPlVQOjc+KBXuR0juNg5nFYsY
0ZcK0N/W9a/tnkmlshRE7Di71+w3fN1O0
6w9o44t6+aINEICCCA4YcF6zMaT1wefWwX6f+
Rmt5nnhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg01DnwCAC8Qh
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string row AAAAB3Nza
switchxxxxxx(config-pubkey-key)# key-string row C1yc2

14.9 show ip ssh

The show ip ssh Privileged EXEC mode command displays the SSH server configuration.

Syntax
show ip ssh

Parameters
N/A

Command Mode
Privileged EXEC mode
Example

The following example displays the SSH server configuration.

```
switchxxxxxx# show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled with auto-login.
SSH Password Authentication is enabled.
```

Active incoming sessions:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>SSH Username</th>
<th>Version</th>
<th>Cipher</th>
<th>Auth Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.1</td>
<td>John Brown</td>
<td>1.5</td>
<td>3DES</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td>182.20.2.1</td>
<td>Bob Smith</td>
<td>1.5</td>
<td>3DES</td>
<td>Password</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The client address</td>
</tr>
<tr>
<td>SSH Username</td>
<td>The user name</td>
</tr>
<tr>
<td>Version</td>
<td>The SSH version number</td>
</tr>
<tr>
<td>Cipher</td>
<td>The encryption type (3DES, Blowfish, RC4)</td>
</tr>
<tr>
<td>Auth Code</td>
<td>The authentication Code (HMAC-MD5, HMAC-SHA1) or Password</td>
</tr>
</tbody>
</table>

14.10 show crypto key pubkey-chain ssh

The `show crypto key pubkey-chain ssh` Privileged EXEC mode command displays SSH public keys stored on the device.

**Syntax**

```
show crypto key pubkey-chain ssh [username username] [fingerprint {bubble-babble | hex}]
```
Parameters

- **username** *username*—Specifies the remote SSH client username. (Length: 1–48 characters)
- **fingerprint** *(bubble-babble | hex)*—Specifies the fingerprint display format. The possible values are:
  - **bubble-babble**—Specifies that the fingerprint is displayed in Bubble Babble format.
  - **hex**—Specifies that the fingerprint is displayed in hexadecimal format.

Default Configuration

The default fingerprint format is hexadecimal.

Command Mode

Privileged EXEC mode

Example

The following examples display SSH public keys stored on the device.

```
switchxxxxxx# show crypto key pubkey-chain ssh
Username              Fingerprint
---------------------- ------------------------------------------

switchxxxxxx# show crypto key pubkey-chain ssh username bob
Username              Fingerprint
---------------------- ------------------------------------------
```
15 Line Commands

15.1 line

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

Syntax

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

Parameters

- **console**—Enters the terminal line mode.
- **telnet**—Configures the device as a virtual terminal for remote access (Telnet).
- **ssh**—Configures the device as a virtual terminal for secured remote access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the device as a virtual terminal for remote (Telnet) access.

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

15.2 speed

Use the `speed` command in Line Configuration mode to set the line baud rate.

Use the `no` form of this command to restore the default configuration.
Syntax

speed bps

no speed

Parameters

bps—Specifies the baud rate in bits per second (bps). Possible values are 4800, 9600, 19200, 38400, 57600, and 115200.

Default Configuration

The default speed is 115200 bps.

Command Mode

Line Configuration mode

User Guidelines

The configured speed is only applied when autobaud is disabled. This configuration applies to the current session only.

Example

The following example configures the line baud rate as 9600 bits per second.

switchxxxxxx(config-line)# speed 9600

15.3 autobaud

Use the autobaud command in Line Configuration mode to configure the line for automatic baud rate detection (autobaud).

Use the no form of this command to disable automatic baud rate detection.

Syntax

autobaud

no autobaud

Default Configuration

Automatic baud rate detection is enabled.
Command Mode
Line Configuration mode

User Guidelines
When this command is enabled, it is activated as follows: connect the console to
the device and press the Enter key twice. The device detects the baud rate
automatically.

Example
The following example enables autobaud.

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

### 15.4 exec-timeout

The `exec-timeout` Line Configuration mode command sets the session idle time
interval, during which the system waits for user input before automatic logoff. Use
the `no` form of this command to restore the default configuration.

**Syntax**

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

**Parameters**

- `minutes`—Specifies the number of minutes. (Range: 0-65535)
- `seconds`—Specifies the number of seconds. (Range: 0-59)

**Default Configuration**

The default idle time interval is 10 minutes.

**Command Mode**
Line Configuration mode
Example
The following example sets the telnet session idle time interval before automatic logoff to 20 minutes and 10 seconds.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# exec-timeout 20 10
```

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

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

Parameters
- `console`—Displays the console configuration.
- `telnet`—Displays the Telnet configuration.
- `ssh`—Displays the SSH configuration.

Default Configuration
If the line is not specified, all line configuration parameters are displayed.

Command Mode
EXEC mode

Example
The following example displays the line configuration.

```
switchxxxxxx# show line
Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
```
Databits: 8
Parity: none
Stopbits: 1

Telnet configuration:
Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10

SSH configuration:
SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
### 16.1 bonjour enable

Use the `bonjour enable` Global Configuration mode command to enable Bonjour globally. Use the `no` format of the command to disable globally.

**Syntax**

```
bonjour enable
no bonjour enable.
```

**Default Configuration**

Enable

**Command Mode**

Global Configuration mode

**Examples**

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

### 16.2 bonjour interface range

Use the `bonjour interface range` Global Configuration mode command to add L2 interfaces to the Bonjour L2 Interface List. Use the `no` format of the command to remove L2 interfaces from the list.

**Syntax**

```
bonjour interface range {interface-list}
```

**Parameters**

- `interface-list`—Specifies a list of interfaces, which can be of the following types:
  - Ethernet port
  - Port-channel
Bonjour Commands

- VLAN

Default Configuration
The list is empty.

Command Mode
Global Configuration mode

User Guidelines
This command can only be used if the device is in Layer 3 (router) mode.

Examples

```
switchxxxxxx(config)# bonjour interface range gi1-3
```

### 16.3 show bonjour

Use the `show bonjour` Privileged EXEC mode command to display Bonjour information

**Syntax**

```
show bonjour [interface-id]
```

**Parameters**

- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel
  - VLAN

**Command Mode**

Privileged EXEC mode
## Examples

### Layer 2:
```
switchxxxxxx# show bonjour

Bonjour status: enabled
L2 interface status: Up
IP Address: 10.5.226.46

<table>
<thead>
<tr>
<th>Service</th>
<th>Admin Status</th>
<th>Oper Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>csco-sb</td>
<td>enabled</td>
<td>enabled</td>
</tr>
<tr>
<td>http</td>
<td>enabled</td>
<td>enabled</td>
</tr>
<tr>
<td>https</td>
<td>enabled</td>
<td>disabled</td>
</tr>
<tr>
<td>ssh</td>
<td>enabled</td>
<td>disabled</td>
</tr>
<tr>
<td>telnet</td>
<td>enabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>
```

### Layer 3:
```
switchxxxxxx# show bonjour

Bonjour global status: enabled
Bonjour L2 interfaces port list: vlans 1

<table>
<thead>
<tr>
<th>Service</th>
<th>Admin Status</th>
<th>Oper Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>csco-sb</td>
<td>enabled</td>
<td>enabled</td>
</tr>
<tr>
<td>http</td>
<td>enabled</td>
<td>enabled</td>
</tr>
<tr>
<td>https</td>
<td>enabled</td>
<td>disabled</td>
</tr>
<tr>
<td>ssh</td>
<td>enabled</td>
<td>disabled</td>
</tr>
<tr>
<td>telnet</td>
<td>enabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>
17.1 aaa authentication login

Use the `aaa authentication login` Global Configuration mode command to set one or more authentication methods to be applied during login. A list of authentication methods may be assigned a list name, and this list name can be used in `aaa authentication enable`. Use the `no` form of this command to restore the default authentication method.

**Syntax**

`aaa authentication login {default | list-name} method1 [method2...]`

`aaa authentication login list-name method1 method2...`

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

**Parameters**

- **default**—Uses the authentication methods that follow this argument as the default method list when a user logs in (this list is unnamed).

- **list-name**—Specifies a name of a list of authentication methods activated when a user logs in. (Length: 1–12 characters)

- **method1 [method2...]**—Specifies a 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:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>Uses the locally-defined usernames for authentication.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>
Default Configuration

If no methods are specified, the default are the locally-defined users and passwords. This is the same as entering the command `aaa authentication login local`.

**NOTE**

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

Command Mode

Global Configuration mode

User Guidelines

Create a list of authentication methods by entering this command with the `list-name` parameter where `list-name` is any character string. The method arguments identifies the list of methods that the authentication algorithm tries, in the given sequence.

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

`no aaa authentication login list-name` deletes a list-name only if it has not been referenced by another command.

Example

The following example sets the authentication login methods for the console.

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

### 17.2 aaa authentication enable

The `aaa authentication enable` Global Configuration mode command sets one or more authentication methods for accessing higher privilege levels. A user, who
logons with a lower privilege level, must pass these authentication methods to access a higher level.

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

Syntax

```
aaa authentication enable {default | list-name} method [method2...]
```

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

Parameters

- **default**—Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.

- **list-name** — Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)

- **method [method2...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. 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:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

Default Configuration

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

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

Global Configuration mode

User Guidelines

Create a list by entering the `aaa authentication enable list-name method1 [method2...]` command where `list-name` is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created by this command are used with `enable authentication`.

All `aaa authentication enable` requests sent by the device to a RADIUS server include the username `$enabx$`, where `x` is the requested privilege level.

All `aaa authentication enable` requests sent by the device to a TACACS+ server include the username that is entered for login authentication.

The additional methods of authentication 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.

`no aaa authentication enable list-name` deletes 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
```

17.3 login authentication

The `login authentication` Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the `no` form of this command to restore the default authentication method.

Syntax

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

Parameters

- **default**—Uses the default list created with the `aaa authentication login` command.
- **list-name**—Uses the specified list created with `aaa authentication login`.

Default Configuration

The default is the `aaa authentication login` command default.

Command Mode

Line Configuration mode

Examples

**Example 1** - The following example specifies the login authentication method as the default method for a console session.

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

**Example 2** - The following example sets the authentication login methods for the console as a list of methods.

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

### 17.4 enable authentication

The `enable authentication` Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the `no` form of this command to restore the default authentication method.
Syntax

`enable authentication {default | list-name}`

`no enable authentication`

Parameters

- `default`—Uses the default list created with the `aaa authentication enable` command.
- `list-name`—Uses the specified list created with the `aaa authentication enable` command.

Default Configuration

The default is the `aaa authentication enable` command default.

Command Mode

Line Configuration mode

Examples

Example 1 - The following example specifies the authentication method as the default 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
```

17.5 `ip http authentication`

The `ip http authentication` Global Configuration mode command specifies authentication methods for HTTP server access. Use the `no` form of this command to restore the default authentication method.
Syntax

ip http authentication aaa login-authentication method1 [method2...]  
oip http authentication aaa login-authentication

Parameters

method [method2...]|—Specifies a list of methods that the authentication algorithm tries, in the given sequence. 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:

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

Default Configuration

The local user database is the default authentication login method. This is the same as entering the ip http authentication local command.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for HTTP and HTTPS server users.

Example

The following example specifies the HTTP access authentication methods.

```
switchxxxxxx(config)# ip http authentication aaa login-authentication radius local none
```
17.6  show authentication methods

The `show authentication methods` Privileged EXEC mode command displays information about the authentication methods.

Syntax

```
show authentication methods
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the authentication configuration.

```
switchxxxxxx# show authentication methods
Login Authentication Method Lists
-----------------------------
Default: Radius, Local, Line
Console_Login: Line, None
Enable Authentication Method Lists
-----------------------------
Default: Radius, Enable
Console_Enable: Enable, None

<table>
<thead>
<tr>
<th>Method</th>
<th>Login Method List</th>
<th>Enable Method List</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console</td>
<td>Console_Login</td>
<td>Console_Enable</td>
</tr>
<tr>
<td>Telnet</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>SSH</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>HTTP:</td>
<td>Radius, local</td>
<td></td>
</tr>
<tr>
<td>HTTPS:</td>
<td>Radius, local</td>
<td></td>
</tr>
<tr>
<td>Dot1x:</td>
<td>Radius</td>
<td></td>
</tr>
</tbody>
</table>
```
17.7 password

Use the `password` Line Configuration mode command to specify a password on a line (also known as an access method, such as a console or Telnet). Use the `no` form of this command to return to the default password.

**Syntax**

```
password password [encrypted]
no password
```

**Parameters**

- `password`—Specifies the password for this line. (Length: 0–159 characters)
- `encrypted`—Specifies that the password is encrypted and copied from another device configuration.

**Default Configuration**

No password is defined.

**Command Mode**

Line Configuration mode

**Example**

The following example specifies the password ‘secret’ on a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secret
```

17.8 enable password

Use the `enable password` Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the `no` form of this command to return to the default password.

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 (for instance, switch B) to another switch (for instance, 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.

**Syntax**

`enable password [level privilege-level] [unencrypted-password | encrypted encrypted-password]`

`no enable password [level level]`

**Parameters**

- `level privilege-level`—Level for which the password applies. If not specified the level is 15. (Range: 1–15)

- `password unencrypted-password`—Password for this level. (Range: 0–159 chars)

- `password encrypted encrypted-password`—Specifies that the password is encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)

**Default Configuration**

Default for `level` is 15.

Passwords are encrypted by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

Passwords are encrypted by default. You only are required to use the `encrypted` keyword when you are actually entering an encrypted keyword.

**Example**

The first command sets an unencrypted password for level 7 (it will be encrypted in the configuration file).
The second command sets a password that has already been encrypted. It will copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# enable password level 7 let-me-in
switchxxxxxx(config)# enable password level 15 encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

### 17.9 service password-recovery

Use the `service password-recovery` Global Configuration mode command to enable the password-recovery mechanism. This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. Use the `no service password-recovery` command to disable the password-recovery mechanism. When the password-recovery mechanism is disabled, accessing the boot menu is still allowed and the user can trigger the password recovery process. The difference is, that in this case, all the configuration files and all the user files are removed. The following log message is generated to the terminal: “All the configuration and user files were removed”.

**Syntax**

```text
service password-recovery
no service password-recovery
```

**Parameters**

N/A

**Default Configuration**

The service password recovery is enabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.
If password recovery is disabled, the user can access the boot menu and trigger the password recovery in the boot menu. The configuration files and user files are removed.

If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

Example

The following command disables password recovery:

```
switchxxxxxx(config)# no service password recovery
```

Note that choosing to use Password recovery option in the Boot Menu during the boot process will remove the configuration files and the user files. Would you like to continue ? Y/N.

### 17.10 username

Use the `username` Global Configuration mode command to establish a username-based authentication system. Use the `no` form to remove a user name.

**Syntax**

```
username name [nopassword | password password | privilege privilege-level | unencrypted-password | encrypted encrypted-password]
username name
no username name
```

**Parameters**

- **name**—The name of the user. (Range: 1–20 characters)
- **nopassword**—No password is required for this user to log in.
- **unencrypted-password**—The authentication password for the user. (Range: 1–159)
- **encrypted encrypted-password**—Specifies that the password is MD5 encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)
- `privilege privilege-level`—Privilege level for which the password applies. If not specified the level is 15. (Range: 1–15).

**Default Configuration**

No user is defined.

**Command Mode**

Global Configuration mode

**Usage Guidelines**

See [User (Privilege) Levels](#) for an explanation of privilege levels.

- The Last level 15 user (regardless of whether it is the default user or any user) cannot be removed.

- Last level 15 user (regardless of whether it is the default user or any user) cannot be demoted

**Examples**

**Example 1** - Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
switchxxxxxx(config)# username tom privilege 15 password 1234
```

**Example 2** - 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 encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

### 17.11 show users accounts

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

**Syntax**

`show user accounts`
Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays information about the users local database.

```
switchxxxxxx# show users accounts
```

<table>
<thead>
<tr>
<th>Username</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>15</td>
</tr>
<tr>
<td>Robert</td>
<td>15</td>
</tr>
<tr>
<td>Smith</td>
<td>15</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The user name.</td>
</tr>
<tr>
<td>Privilege</td>
<td>The user’s privilege level.</td>
</tr>
</tbody>
</table>

17.12 `aaa accounting login`

Use the `aaa accounting login` command in Global Configuration mode to enable accounting of device management sessions.

Use the `no` form of this command to disable accounting of device management sessions.

Syntax

```
aaa accounting login start-stop group {radius | tacacs+}
```

```
no aaa accounting login start-stop
```
Parameters

- radius—Uses a RADIUS server for accounting.
- tacacs+—Uses a TACACS+ server for accounting.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that are identified with a username (e.g. a user that is logged in with a line password is not recorded).

If accounting is activated, the device sends “start/stop” messages to the RADIUS/TACACS+ server when a user logs in/logs out respectively.

The device uses the configured priorities of the available RADIUS/TACACS+ servers to select the RADIUS/TACACS+ server.

The following table describes the supported RADIUS accounting attributes values, and in which messages they are sent by the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Sent in Start Message</th>
<th>Sent in Stop Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name (1)</td>
<td>User’s identity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NAS-IP-Address (4)</td>
<td>The switch IP address that is used for the session with the RADIUS server.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Class (25)</td>
<td>Arbitrary value is included in all accounting packets for a specific session.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Called-Station-ID (30)</td>
<td>The switch IP address that is used for the management session.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Authentication, Authorization and Accounting (AAA) Commands

The following table describes the supported TACAC+ accounting attributes values, and in which messages they are sent by the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Sent in Start Message</th>
<th>Sent in Stop Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling-Station-ID (31)</td>
<td>The user IP address.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Acct-Session-ID (44)</td>
<td>A unique accounting identifier.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Acct-Authentic (45)</td>
<td>Indicates how the supplicant was authenticated.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Acct-Session-Time (46)</td>
<td>Indicates how long the user was logged in.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Acct-Terminate-Cause (49)</td>
<td>Reports why the session was terminated.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The following table describes the supported TACAC+ accounting attributes values, and in which messages they are sent by the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Sent in Start Message</th>
<th>Sent in Stop Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_id</td>
<td>Yes</td>
<td>Yes</td>
<td>A unique accounting session identifier.</td>
</tr>
<tr>
<td>user</td>
<td>Yes</td>
<td>Yes</td>
<td>Username that is entered for login authentication</td>
</tr>
<tr>
<td>rem-addr</td>
<td>Yes</td>
<td>Yes</td>
<td>IP address of the user</td>
</tr>
<tr>
<td>elapsed-time</td>
<td>No</td>
<td>Yes</td>
<td>Indicates how long the user was logged in.</td>
</tr>
<tr>
<td>reason</td>
<td>No</td>
<td>Yes</td>
<td>Reports why the session was terminated.</td>
</tr>
</tbody>
</table>

**Example**

```
switchxxxxxx(config)# aaa accounting login start-stop group tacacs
```

### 17.13  aaa accounting dot1x

To enable accounting of 802.1x sessions, use the `aaa accounting dot1x` Global Configuration mode command. Use the `no` form of this command to disable accounting.
Syntax

aaa accounting dot1x start-stop group radius
no aaa accounting dot1x start-stop group radius

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends a “start”/“stop” messages to a Radius server when a user logs in / logs out to the network, respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

If a new supplicant replaces an old supplicant (even if the port state remains authorized), the software sends a “stop” message for the old supplicant and a “start” message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends “start”/“stop” messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends “start”/“stop” messages only for the supplicant that has been authenticated.

The software does not send “start”/“stop” messages if the port is force-authorized.

The software does not send “start”/“stop” messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.

The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Start</th>
<th>Stop</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name (1)</td>
<td>Yes</td>
<td>Yes</td>
<td>Supplicant’s identity.</td>
</tr>
</tbody>
</table>
Example

switchxxxxxx(config)# aaa accounting dot1x start-stop group radius

17.14 show accounting

The show accounting EXEC mode command displays information about the status of login accounting.

Syntax
show accounting

Parameters
N/A
Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example displays information about the accounting status.

switchxxxxxx# show accounting
Login: TACACS+
802.1x: Disabled

17.15 passwords complexity enable

Use the passwords complexity enable Global Configuration mode command to enforce minimum password complexity. The no form of this command disables enforcing password complexity.

Syntax
passwords complexity enable
no passwords complexity enable

Parameters
N/A

Default Configuration
Enabled

Command Mode
Global Configuration mode

User Guidelines
If password complexity is enabled by default, the user is forced 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).
- Are different from the current password.
- Contains no character that is repeated more than 3 times consecutively.
- Does not repeat or reverse the user name or any variant reached by changing the case of the characters.
- Does not repeat or reverse the manufacturer’s name or any variant reached by changing the case of the characters.

You can control the above attributes of 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 wipe out the other settings. It works only as a toggle.

**Example**

The following example configures requiring complex passwords that fulfill the minimum requirements specified in the User Guidelines above.

```
switchxxxxxx(config)# passwords complexity enable
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
New password must be different than the manufacturer name: Enabled
switchcc293e#
```
17.16 passwords complexity <attributes>

Use the passwords complexity <attributes> Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the no form of these commands to return to default.

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
passwords complexity not-manufacturer-name
no passwords complexity not-manufacturer-name

Parameters

- **min-length number**—Sets the minimal length of the password. (Range: 0–64)
- **min-classes number**—Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 0–4)
- **not-current**—Specifies that the new password cannot be the same as the current password.
- **no-repeat number**—Specifies the maximum number of characters in the new password that can be repeated consecutively. Zero specifies that there is no limit on repeated characters. (Range: 0–16)
not-username—Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.

not-manufacturer-name—Specifies that the password cannot repeat or reverse the manufacturer’s name or any variant reached by changing the case of the characters.

Default Configuration
The minimal length is 8.
The number of classes is 3.
The default for no-repeat is 3.
All the other controls are enabled by default.

Command Mode
Global Configuration mode

Example
The following example configures the minimal required password length to 8 characters.

```
switchxxxxxx (config)# passwords complexity min-length 8
```

17.17 passwords aging
Use the passwords aging Global Configuration mode command to enforce password aging. Use the no form of this command to return to default.

Syntax
```
passwords aging days
no passwords aging
```

Parameters
```
days—Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365)
```
Default Configuration
Enabled and the number of days is 180.

Command Mode
Global Configuration mode

User Guidelines
Aging is relevant only to users of the local database with privilege level 15 and to “enable” a password of privilege level 15.

To disable password aging, use `passwords aging 0`. Using `no passwords aging` sets the aging time to the default.

Example
The following example configures the aging time to be 24 days.

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

17.18 show passwords configuration
The `show passwords configuration` Privileged EXEC mode command displays information about the password management configuration.

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
New password must be different than the manufacturer name: Enabled
switchcc293e#

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal length</td>
<td>The minimal length required for passwords in the local database.</td>
</tr>
<tr>
<td>Minimal character classes</td>
<td>The minimal number of different types of characters (special characters, integers and so on) required to be part of the password.</td>
</tr>
<tr>
<td>Maximum number of repeated characters</td>
<td>The maximum number of times a single character can be repeated in the password.</td>
</tr>
<tr>
<td>Level</td>
<td>The applied password privilege level.</td>
</tr>
<tr>
<td>Aging</td>
<td>The password aging time in days.</td>
</tr>
</tbody>
</table>
RADIUS Commands

18.1 radius-server host

Use the `radius-server host` Global Configuration mode command to configure a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.

Use the `encrypted` form of the command to enter a key in its encrypted form.

Syntax

```
radius-server host {ip-address | hostname} [auth-port auth-port-number] [acct-port acct-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [source {source-ip}] [priority priority] [usage {login | 802.1x | all}]
```

```
encrypted radius-server host {ip-address | hostname} [auth-port auth-port-number] [acct-port acct-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key encrypted-key-string] [source {source-ip}] [priority priority] [usage {login | 802.1x | all}]
```

```
no radius-server host {ip-address | hostname}
```

Parameters

- `ip-address`—Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions
- `hostname`—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)
- `auth-port auth-port-number`—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- `acct-port-number`—Port number for accounting requests. The host is not used for accountings if set to 0. If unspecified, the port number defaults to 1813.
- `timeout timeout`—Specifies the timeout value in seconds. (Range: 1–30)
- `retransmit retries`—Specifies the retransmit value. (Range: 1–10)
- **deadtime** `deadtime`—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)

- **key** `key-string`—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters). If this parameter is omitted, the globally-configured radius key will be used.

- **key** `encrypted-key-string`—same as key-string, but the key is in encrypted format.

- **source** `source-ip`—Specifies the source IPv4 or IPv6 address to use for communication. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

- **priority** `priority`—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)

- **usage** `{login | 802.1x | all}`—Specifies the RADIUS server usage type. The possible values are:
  - **login**—Specifies that the RADIUS server is used for user login parameters authentication.
  - **802.1x**—Specifies that the RADIUS server is used for 802.1x port authentication.
  - **all**—Specifies that the RADIUS server is used for user login authentication and 802.1x port authentication.

- **encrypted-key-string**—Same as the key-string parameter, but the key is in encrypted form.

**Default Configuration**

The default authentication port number is 1812.

If **timeout** is not specified, the global value (set in `radius-server timeout`) is used.

If **retransmit** is not specified, the global value (set in `radius-server retransmit`) is used.

If **key-string** is not specified, the global value (set in `radius-server key`) is used.

If the **source** value is not specified, the global value (set in `radius-server source-ip` or `radius-server source-ipv6`) 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 `radius-server timeout`, the default timeout for `radius-server timeout` is used.

The default usage type is all.

**Command Mode**

Global Configuration mode

**User Guidelines**

To specify multiple hosts, this command is used for each host.

The `source` parameter address type (IPv4 or IPv6) must be the same as that of the `host` IP address type.

**Example**

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
switchxxxxxx(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

### 18.2 radius-server key

Use the `radius-server key` Global Configuration mode command to set the authentication and encryption key for RADIUS communications between the device and the RADIUS daemon.

Use the `no` form of this command to restore the default configuration.

**Syntax**

```
radius-server key [key-string]
encrypted radius-server key [encrypted-key-string]
no radius-server key
```

**Parameters**

- `key-string`—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must
match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

- **encrypted-key-string**—Same as the key-string parameter, but the key is in encrypted form.

**Default Configuration**

The key-string is an empty string.

**Command Mode**

Global Configuration mode

**Example**

The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
switchxxxxxx(config)# radius-server key enterprise-server
```

### 18.3 radius-server retransmit

Use the `radius-server retransmit` Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

**Syntax**

```
radius-server retransmit retries
no radius-server retransmit
```

**Parameters**

- **retransmit retries**—Specifies the retransmit value. (Range: 1–10)

**Default Configuration**

The software searches the list of RADIUS server hosts 3 times.

**Command Mode**

Global Configuration mode
Example

The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
switchxxxxxx(config)# radius-server retransmit 5
```

18.4 radius-server source-ip

Use the `radius-server source-ip` Global Configuration mode command to specify the source IP address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

**Syntax**

```
radius-server source-ip {source-ip-address}
no radius-server source-ip {source-ip-address}
```

**Parameters**

- `source-ip-address`—Specifies the source IP address.

**Default Configuration**

The source IP address is the IP address of the outgoing IP interface.

**Command Mode**

Global Configuration mode

**User Guidelines**

If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

**Example**

The following example configures the source IP address used for communication with all RADIUS servers to 10.1.1.1.

```
switchxxxxxx(config)# radius-server source-ip 10.1.1.1
```
18.5 radius-server source-ipv6

Use the radius-server source-ipv6 Global Configuration mode command to specify the source IPv6 address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

radius-server source-ipv6 {source}
no radius-server source-ipv6 {source}

Parameters

source—Specifies the source IPv6 address.

Default Configuration

The source IP address is the IP address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

Example

The following example configures the source IP address used for communication with all RADIUS servers to 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

```
switchxxxxxx(config)# radius-server source-ipv6
```

18.6 radius-server timeout

Use the radius-server timeout Global Configuration mode command to set how long the device waits for a server host to reply. Use the no form of this command to restore the default configuration.
RADIUS Commands

278  78-21075-01  Command Line Interface Reference Guide

18

Syntax
radius-server timeout  timeout-seconds
no radius-server timeout

Parameters
timeout  timeout-seconds—Specifies the timeout value in seconds. (Range: 1–30)

Default Configuration
The default timeout value is 3 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the timeout interval on all RADIUS servers to 5 seconds.

switchxxxxxxx(config)# radius-server timeout 5

18.7  radius-server deadtime

Use the radius-server deadtime Global Configuration mode command to configure how long unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the no form of this command to restore the default configuration.

Syntax
radius-server deadtime  deadtime
no radius-server deadtime

Parameters
deadtime—Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)

Default Configuration
The default deadtime interval is 0.
Command Mode
Global Configuration mode

Example
The following example sets all RADIUS server deadtimes to 10 minutes.

```
switchxxxxxx(config)# radius-server deadtime 10
```

18.8 show radius-servers
Use the `show radius-servers` Privileged EXEC mode command to display the RADIUS server settings.

Syntax
```
show radius-servers
```

Command Mode
Privileged EXEC mode

Example
The following example displays RADIUS server settings:

```
switchxxxxxx# show radius-servers

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>Port</th>
<th>Time</th>
<th>Deadtime</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.1</td>
<td>1812</td>
<td>1813</td>
<td>Global</td>
<td>Global</td>
<td>1</td>
</tr>
<tr>
<td>172.16.1.2</td>
<td>1812</td>
<td>1813</td>
<td>11</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>

Global values
-------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
18.9 show radius-servers key

Use the show radius-servers key Privileged EXEC mode command to display the RADIUS server key settings.

Syntax
show radius-servers key

Command Mode
Privileged EXEC mode

Example
The following example displays RADIUS server key settings.

```
switchxxxxxx# show radius-servers key
IP address       Key (Encrypted)
--------------------------------------
172.16.1.1        sdfsdkj1koi5jdoiklsjdf

Global key (Encrypted)
----------------------
sdklfjdljfwkljksdj
```
TACACS+ Commands

19.1 tacacs-server host

Use the **tacacs-server host** Global Configuration mode command to specify a TACACS+ host. Use the **no** form of this command to delete the specified TACACS+ host.

**Syntax**

```
tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source {source-ip}] [priority priority]
```

```
encrypted tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key encrypted-key-string] [source {source-ip}] [priority priority]
```

```
no tacacs-server host {ip-address | hostname}
```

**Parameters**

- **host ip-address**—Specifies the TACACS+ server host IP address. Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.
- **host hostname**—Specifies the TACACS+ server host name. (Length: 1-158 characters. Maximum label length of each part of the host name: 63 characters)
- **single-connection**—Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- **port port-number**—Specifies the TACACS server TCP port number. If the port number is 0, the host is not used for authentication. (Range: 0-65535)
- **timeout timeout**—Specifies the timeout value in seconds. (Range: 1-30)
- **key key-string**—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0-128 characters). If this parameter is omitted, the globally-defined key (set in **tacacs-server key**) will be used.
• **key encrypted-key-string**—Same as key-string, but the key is in encrypted format.

• **source source-ip**—Specifies the source IPv4 or IPv6 address to use for communication. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

• **priority priority**—Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

**Default Configuration**

No TACACS+ host is specified.

The default authentication port number is 1812.

If **timeout** is not specified, the global value (set in `tacacs-server timeout`) is used.

If **key-string** is not specified, the global value (set in `tacacs-server key`) is used.

If the **source** value is not specified, the global value (set in `tacacs-server source-ip` or `tacacs-server source-ipv6`) 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 `tacacs-server timeout`, the default timeout for `tacacs-server timeout` is used.

**Command Mode**

Global Configuration mode

**User Guidelines**

Multiple `tacacs-server host` commands can be used to specify multiple hosts.

**Example**

The following example specifies a TACACS+ host.

```
switchxxxxxx(config)# tacacs-server host 172.16.1.1
```

**19.2 tacacs-server key**

Use the **tacacs-server key** Global Configuration mode command to set the authentication encryption key used for all TACACS+ communications between the
device and the TACACS+ daemon. Use the no form of this command to disable the key.

Syntax

tacacs-server key key-string

encrypted tacacs-server key encrypted-key-string

no tacacs-server key

Parameters

- **key-string**—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)

- **encrypted-key-string**—Same as key-string, but the key is in encrypted format.

Default Configuration

The default key is an empty string.

Command Mode

Global Configuration mode

Example

The following example sets Enterprise as the authentication encryption key for all TACACS+ servers.

```
switchxxxxx(config)# tacacs-server key enterprise
```

### 19.3 tacacs-server timeout

Use the `tacacs-server timeout` Global Configuration mode command to set the interval during which the device waits for a TACACS+ server to reply. Use the no form of this command to restore the default configuration.

Syntax

tacacs-server timeout timeout
### no tacacs-server timeout

**Parameters**

**timeout**—Specifies the timeout value in seconds. (Range: 1-30)

**Default Configuration**

The default timeout value is 5 seconds.

**Command Mode**

Global Configuration mode

**Example**

The following example sets the timeout value to 30 for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server timeout 30
```

### 19.4 tacacs-server source-ip

Use the **tacacs-server source-ip** Global Configuration mode command to configure the source IP address to be used for communication with TACACS+ servers. Use the no form of this command to restore the default configuration.

**Syntax**

```
tacacs-server source-ip {source}
no tacacs-server source-ip {source}
```

**Parameters**

**source**—Specifies the source IP address. (Range: Valid IP address)

**Default Configuration**

The default source IP address is the outgoing IP interface address.

**Command Mode**

Global Configuration mode
**User Guidelines**

If the configured IP source address has no available IP interface, an error message is issued when attempting to communicate with the IP address.

**Example**

The following example specifies the source IP address for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server source-ip 172.16.8.1
```

### 19.5 `tacacs-server source-ipv6`

Use the `tacacs-server source-ipv6` Global Configuration mode command to configure the source IPv6 address to be used for communication with TACACS+ servers.

Use the `no` form of this command to restore the default configuration.

**Syntax**

```
tacacs-server source-ipv6 {source}
no tacacs-server source-ipv6 {source}
```

**Parameters**

- **source**—Specifies the source IPv6 address.

**Default Configuration**

The default source IP address is the outgoing IP interface address.

**Command Mode**

Global Configuration mode

**User Guidelines**

If the configured IP source address has no available IP interface, an error message is issued when attempting to communicate with the IP address.
Example
The following example specifies the source IP address for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server source-ipv6
```

19.6 show tacacs
Use the **show tacacs** Privileged EXEC mode command to display configuration and statistical information for a TACACS+ server.

**Syntax**
```
show tacacs [ip-address]
```

**Parameters**
- **ip-address**—Specifies the TACACS+ server name, IP or IPv6 address.

**Default Configuration**
If **ip-address** is not specified, information for all TACACS+ servers is displayed.

**Command Mode**
Privileged EXEC mode

**Example**
The following example displays configuration and statistical information for all TACACS+ servers.

```
switchxxxxxx# show tacacs

<table>
<thead>
<tr>
<th>IP address</th>
<th>Status</th>
<th>Port</th>
<th>Single Connection</th>
<th>Time Out</th>
<th>Source IP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.1</td>
<td>Connected</td>
<td>49</td>
<td>No</td>
<td>Global</td>
<td>Global</td>
<td>1</td>
</tr>
</tbody>
</table>

Global values

Time Out: 3
Source IP: 172.16.8.1
```
19.7 show tacacs key

Use the show tacacs key Privileged EXEC mode command to display the configured key of the TACACS+ server.

Syntax

show tacacs key [ip-address]

Parameters

ip-address—Specifies the TACACS+ server name or IP address.

Default Configuration

If ip-address is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays configuration and statistical information for all TACACS+ servers.

```
switchxxxxxx# show tacacs key

IP address                      Key (Encrypted)

Global key (Encrypted)

-----------
```
20.1 logging on

Use the **logging on** Global Configuration mode command to control error message logging. This command sends debug or error messages asynchronously to designated locations. Use the **no** form of this command to disable the logging.

**Syntax**

```
logging on
no logging on
```

**Parameters**

N/A

**Default Configuration**

Message logging is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

The logging process controls the logging messages 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 buffered`, `logging file`, and `logging on` Global Configuration mode commands. However, if the `logging on` command is disabled, no messages are sent to these destinations. Only the console receives messages.

**Example**

The following example enables logging error messages.

```
switchxxxxxx(config)# logging on
```
20.2 logging host

Use the `logging host` Global Configuration command to log messages to the specified SYSLOG server. Use the `no` form of this command to delete the SYSLOG server with the specified address from the list of SYSLOG servers.

Syntax

```
logging host {ip-address | ipv6-address | hostname} [port port] [severity level] [facility facility] [description text]
no logging host {ipv4-address | ipv6-address | hostname}
```

Parameters

- **ip-address**—IP address of the host to be used as a SYSLOG server. The IP address can be an IPv4, IPv6 or Ipv6z address. See IPv6z Address Conventions.
- **hostname**—Hostname of the host to be used as a SYSLOG server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size for each part of the host name: 63)
- **port port**—Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- **severity level**—Limits the logging of messages to the SYSLOG servers to a specified level: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.
- **facility facility**—The facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7. If unspecified, the port number defaults to local7.
- **description text**—Description of the SYSLOG server. (Range: Up to 64 characters)

Default Configuration

No messages are logged to a SYSLOG server.

If unspecified, the **severity level** defaults to Informational.

Command Mode

Global Configuration mode
User Guidelines

You can use multiple SYSLOG servers.

Examples

```plaintext
switchxxxxxx(config)# logging host 1.1.1.121
```

```plaintext
switchxxxxxx(config)# logging host 3000::100/SYSLOG1
```

20.3 logging console

Use the **logging console** Global Configuration mode command to limit messages logged to the console to messages to a specific severity level. Use the no form of this command to restore the default.

Syntax

- `logging console level`

- `no logging console`

Parameters

- **level**—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

Informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages displayed on the console to messages with severity level **errors**.

```plaintext
switchxxxxxxx(config)# logging console errors
```
20.4 logging buffered

Use the `logging buffered` Global Configuration mode command to limit the SYSLOG message display to messages with a specific severity level, and to define the buffer size (number of messages that can be stored). Use the `no` form of this command to cancel displaying the SYSLOG messages, and to return the buffer size to default.

**Syntax**

```
logging buffered [buffer-size] [severity-level | severity-level-name]
no logging buffered
```

**Parameters**

- **buffer-size**—Specifies the maximum number of messages stored in the history table. (Range: 20–400)
- **severity-level**—Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- **severity-level-name**—Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

**Default Configuration**

The default severity level is informational.

The default buffer size is 200.

**Command Mode**

Global Configuration mode

**User Guidelines**

All the SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

**Example**

The following example shows two ways of limiting the SYSLOG message display from an internal buffer to messages with severity level `debugging`. In the second example, the buffer size is set to 100.
20.5 clear logging

Use the clear logging Privileged EXEC mode command to clear messages from the internal logging buffer.

Syntax

```
clear logging
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

```
switchxxxxxx# clear logging
Clear logging buffer [confirm]
```

20.6 logging file

Use the logging file Global Configuration mode command to limit SYSLOG messages sent to the logging file to messages with a specific severity level. Use the no form of this command to cancel sending messages to the file.

Syntax

```
logging file level
no logging file
```
Parameters

level—Specifies the severity level of SYSLOG messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is errors.

Command Mode

Global Configuration mode

Example

The following example limits SYSLOG messages sent to the logging file to messages with severity level alerts.

```
switchxxxxxx(config)# logging file alerts
```

20.7 clear logging file

Use the clear logging file Privileged EXEC mode command to clear messages from the logging file.

Syntax

clear logging file

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode
Example
The following example clears messages from the logging file.

```
switchxxxxxx# clear logging file
Clear Logging File [y/n]
```

## 20.8 aaa logging

Use the `aaa logging` Global Configuration mode command to enable logging of the logins of authenticated users.

Use the `no` form of this command to disable logging of authenticated users.

**Syntax**

```
aaa logging {login}
no aaa logging {login}
```

**Parameters**

`login`—Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

**Default Configuration**

Enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of authenticated user events are not subject to this command.

**Example**

The following example enables logging of authenticated users.

```
switchxxxxxx(config)# aaa logging login
```
20.9 file-system logging

Use the `file-system logging` Global Configuration mode command to enable logging file system events. Use the `no` form of this command to disable logging file system events.

**Syntax**

```
file-system logging {copy / delete-rename}
```

```
no file-system logging {copy / delete-rename}
```

**Parameters**

- `copy`—Specifies logging messages related to file copy operations.
- `delete-rename`—Specifies logging messages related to file deletion and renaming operations.

**Default Configuration**

Enabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables logging messages related to file copy operations.

```
switchxxxxxx(config)# file-system logging copy
```

20.10 logging aggregation on

Use the `logging aggregation on` Global Configuration mode command to control aggregation of SYSLOG messages. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by `logging aggregation aging-time`). Use the `no` form of this command to disable aggregation of SYSLOG messages.

**Syntax**

```
logging aggregation on
```

```
no logging aggregation on
```
no logging aggregation on

Parameters
N/A

Default Configuration
Enabled.

Command Mode
Global Configuration mode

Example
To turn off aggregation of SYSLOG messages:

```
switchxxxxxx(config)# no logging aggregation on
```

### 20.11 logging aggregation aging-time

Use the `logging aggregation aging-time` Global Configuration mode command to configure the aging time of the aggregated SYSLOG messages. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. Use the `no` form of this command to return to the default.

**Syntax**

- `logging aggregation aging-time sec`
- `no logging aggregation aging-time`

**Parameters**

- `aging-time sec`—Aging time in seconds (Range: 15–3600)

**Default Configuration**

300 seconds.

**Command Mode**

Global Configuration mode
Example

switchxxxxxx(config)# logging aggregation aging-time 300

20.12 logging origin-id

Use the logging origin-id Global Configuration mode command to configure the origin field of the SYSLOG message packet headers sent to the SYSLOG server. Use the no form of this command to return to the default.

Syntax

logging origin-id {hostname | IP | IPv6 | string user-defined-id}
no logging origin-id

Parameters

- hostname—Message origin identifier.
- IP—IP address of the sending interface that is used as the message origin identifier.
- IPv6—IPv6 address of the sending interface that is used as the message origin identifier. If the sending interface is IPv4, the IPv4 address will be used instead.
- string user-defined-id—Specifies an identifying description chosen by the user. The user-defined-id argument is the identifying description string.

Default Configuration

No header is send apart from PRI field.

Command Mode

Global Configuration mode

Example

switchxxxxxx(config)# logging origin-id string “Domain 1, router B”
20.13  show logging

Use the `show logging` Privileged EXEC mode command to display the logging status and SYSLOG messages stored in the internal buffer.

**Syntax**

```
show logging
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example displays the logging status and the SYSLOG messages stored in the internal buffer.

```
switchxxxxx# show logging
Logging is enabled.
Origin id: hostname
Console Logging: Level info. Console Messages: 0 Dropped.
4 messages were not logged
Application filtering control

<table>
<thead>
<tr>
<th>Application</th>
<th>Event</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Login</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Copy</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Delete-Rename</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
Management ACL  Deny  Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up: Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up: SYSLOG6
01-Jan-2010 05:29:02 :%LINK-I-Up: SYSLOG7
01-Jan-2010 05:29:00 :%LINK-W-Down: SYSLOG8

20.14 show logging file
Use the show logging file Privileged EXEC mode command to display the logging status and the SYSLOG messages stored in the logging file.

Syntax
show logging file

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the logging status and the SYSLOG messages stored in the logging file.

switchxxxxxx# show logging file
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
4 messages were not logged

Application filtering control

<table>
<thead>
<tr>
<th>Application</th>
<th>Event</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Login</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Copy</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Delete-Rename</td>
<td>Enabled</td>
</tr>
<tr>
<td>Management ACL</td>
<td>Deny</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Aggregation: Disabled.
Aggregation aging time: 300 Sec

01-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob bgEgGnt9z6NHgZwKt5xKqF7cBtd11xmFgSEWuDhho5UedydAjVkJ5SXR2... failed
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key type.
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 != SIGBLOB_LEN

20.15 show syslog-servers

Use the show syslog-servers Privileged EXEC mode command to display the SYSLOG server settings.

Syntax

show syslog-servers

Parameters

N/A
Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example provides information about the SYSLOG servers.

switchxxxxxx# show syslog-servers

Device Configuration

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>Facility</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.121</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td></td>
</tr>
<tr>
<td>3000::100</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td></td>
</tr>
</tbody>
</table>
21 Remote Network Monitoring (RMON) Commands

21.1 show rmon statistics

Use the show rmon statistics EXEC mode command to display RMON Ethernet statistics.

Syntax

show rmon statistics {interface-id}

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays RMON Ethernet statistics for gigabitethernet port gi1.

```
switchxxxxxx# show rmon statistics gi1
Port gi1
Dropped: 0
Octets: 0 Packets: 0
Broadcast: 0 Multicast: 0
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 0 65 to 127 Octets: 1
128 to 255 Octets: 1 256 to 511 Octets: 1
512 to 1023 Octets: 0 1024 to max Octets: 0
```
The following table describes the significant fields displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped</td>
<td>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 this condition was detected.</td>
</tr>
<tr>
<td>Octets</td>
<td>Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>Total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Total number of good packets received and directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>CRC Align Errors</td>
<td>Total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Collisions</td>
<td>Best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Undersize Pkts</td>
<td>Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Oversize Pkts</td>
<td>Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
</tbody>
</table>
Remote Network Monitoring (RMON) Commands

21.2 rmon collection stats

Use the `rmon collection stats` Interface Configuration mode command to enable RMON MIB collecting history statistics (in groups) on an interface. Use the `no` form of this command to remove a specified RMON history group of statistics.

Syntax

```
rmon collection stats index [owner ownername] [buckets bucket-number] [interval seconds]

no rmon collection stats index
```

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jabbers</td>
<td>Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>64 Octets</td>
<td>Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>65 to 127 Octets</td>
<td>Total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>128 to 255 Octets</td>
<td>Total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>256 to 511 Octets</td>
<td>Total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>512 to 1023 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>1024 to max</td>
<td>Total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
Parameters

- **index**—The requested group of statistics index. (Range: 1–65535)
- **owner ownername**—Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string. (Range: Valid string)
- **buckets bucket-number**—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1–50)
- **interval seconds**—The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

Command Mode

Interface Configuration (Ethernet, Port-channel) mode. Cannot be configured for a range of interfaces (range context).

### 21.3 show rmon collection stats

Use the `show rmon collection stats` EXEC mode command to display the requested RMON history group statistics.

**Syntax**

```
show rmon collection stats [interface-id]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode
Example

The following example displays all RMON history group statistics.

```
switchxxxxxx# show rmon collection stats
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Interface</th>
<th>Interval</th>
<th>Requested Samples</th>
<th>Granted Samples</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>gi1</td>
<td>30</td>
<td>50</td>
<td>50</td>
<td>CLI</td>
</tr>
<tr>
<td>2</td>
<td>gi1</td>
<td>1800</td>
<td>50</td>
<td>50</td>
<td>Manager</td>
</tr>
</tbody>
</table>

The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The sampled Ethernet interface.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds between samples.</td>
</tr>
<tr>
<td>Requested Samples</td>
<td>The requested number of samples to be saved.</td>
</tr>
<tr>
<td>Granted Samples</td>
<td>The granted number of samples to be saved.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>

21.4 show rmon history

Use the `show rmon history` EXEC mode command to display RMON Ethernet history statistics.

**Syntax**

```
show rmon history index {throughput | errors | other} [period seconds]
```

**Parameters**

- `index`—Specifies the set of samples to display. (Range: 1–65535)
- `throughput`—Displays throughput counters.
- `errors`—Displays error counters.
- `other`—Displays drop and collision counters.
- **period seconds**—Specifies the period of time in seconds to display.
  (Range: 1–2147483647)

**Command Mode**

**EXEC mode**

**Example**

The following examples display RMON Ethernet history statistics for index 1

```
switchxxxxxx# show rmon history 1 throughput
Sample Set: 1 Owner: CLI
Interface: gi1 Interval: 1800
Requested samples: 50  Granted samples: 50
Maximum table size: 500

<table>
<thead>
<tr>
<th>Time</th>
<th>Octets</th>
<th>Packets</th>
<th>Broadcast</th>
<th>Multicast</th>
<th>Util</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18 2005 21:57:00</td>
<td>303595962</td>
<td>357568</td>
<td>3289</td>
<td>7287</td>
<td>19%</td>
</tr>
<tr>
<td>Jan 18 2005 21:57:30</td>
<td>287696304</td>
<td>275686</td>
<td>2789</td>
<td>5878</td>
<td>20%</td>
</tr>
</tbody>
</table>
```

```
switchxxxxxx# show rmon history 1 errors
Sample Set: 1 Owner: Me
Interface:gi1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500 (800 after reset)

<table>
<thead>
<tr>
<th>Time</th>
<th>CRC</th>
<th>Under</th>
<th>Oversize</th>
<th>Fragments</th>
<th>Jabbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18 2005 21:57:00</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>49</td>
<td>0</td>
</tr>
<tr>
<td>Jan 18 2005 21:57:30</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>27</td>
<td>0</td>
</tr>
</tbody>
</table>
```
switchxxxxxx# show rmon history 1 other
Sample Set: 1 Owner: Me
Interface: gi1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500

<table>
<thead>
<tr>
<th>Time</th>
<th>Dropped</th>
<th>Collisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18 2005 21:57:00</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Jan 18 2005 21:57:30</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and Time the entry is recorded.</td>
</tr>
<tr>
<td>Octets</td>
<td>Total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets (including bad packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Number of good packets received during this sampling interval that were directed to the broadcast address.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
<tr>
<td>CRC Align</td>
<td>Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Undersize</td>
<td>Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
</tbody>
</table>
21.5  rmon alarm

Use the `rmon alarm` Global Configuration mode command to configure alarm conditions. Use the `no` form of this command to remove an alarm.

Syntax

```
rmon alarm index mib-object-id interval rising-threshold falling-threshold rising-event falling-event [type {absolute | delta}] [startup {rising | rising-falling | falling}] [owner name]
```

no rmon alarm index

Parameters

- **index**—Specifies the alarm index. (Range: 1–65535)
- **mib-object-id**—Specifies the object identifier of the variable to be sampled. (Valid OID)

- **interval**—Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1–4294967295)

- **rising-threshold**—Specifies the rising threshold value. (Range: 0–4294967295)

- **falling-threshold**—Specifies the falling threshold value. (Range: 0–4294967295)

- **rising-event**—Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)

- **falling-event**—Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)

- **type {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**—Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.
  - **delta**—Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.

- **startup {rising | rising-falling | falling}**—Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - **rising**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rising-threshold**, a single rising alarm is generated.
  - **rising-falling**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rising-threshold**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to **falling-threshold**, a single falling alarm is generated.
  - **falling**—Specifies that if the first sample (after this entry becomes valid) is less than or equal to **falling-threshold**, a single falling alarm is generated.

- **owner name**—Specifies the name of the person who configured this alarm. (Valid string)
Default Configuration

The default method type is **absolute**.

The default **startup** direction is **rising-falling**.

If the owner **name** is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an alarm with index 1000, MIB object ID D-Link, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
switchxxxxxx(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20
```

21.6  **show rmon alarm-table**

Use the **show rmon alarm-table** EXEC mode command to display a summary of the alarms table.

Syntax

```
show rmon alarm-table
```

Command Mode

EXEC mode
Example

The following example displays the alarms table.

```
switchxxxxxx# show rmon alarm-table
```

<table>
<thead>
<tr>
<th>Index</th>
<th>OID</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.3.6.1.2.1.2.2.1.10.1</td>
<td>CLI</td>
</tr>
<tr>
<td>2</td>
<td>1.3.6.1.2.1.2.2.1.10.1</td>
<td>Manager</td>
</tr>
<tr>
<td>3</td>
<td>1.3.6.1.2.1.2.2.1.10.9</td>
<td>CLI</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>

21.7 show rmon alarm

Use the `show rmon alarm` EXEC mode command to display alarm configuration.

**Syntax**

show rmon alarm `number`

**Parameters**

alarm `number`—Specifies the alarm index. (Range: 1–65535)

**Command Mode**

EXEC mode

**Example**

The following example displays RMON 1 alarms.

```
switchxxxxxx# show rmon alarm 1
Alarm 1
```
------

OID: 1.3.6.1.2.1.2.2.2.1.10.1  
Last sample Value: 878128  
Interval: 30  
Sample Type: delta  
Startup Alarm: rising  
Rising Threshold: 8700000  
Falling Threshold: 78  
Rising Event: 1  
Falling Event: 1  
Owner: CLI

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Alarm index.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Last Sample Value</td>
<td>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.</td>
</tr>
<tr>
<td>Interval</td>
<td>Interval in seconds over which the data is sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>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.</td>
</tr>
</tbody>
</table>
21.8 rmon event

Use the `rmon event` Global Configuration mode command to configure an event. Use the `no` form of this command to remove an event.

Syntax

```
rmon event index [none | log | trap | log-trap] [community text] [description text] [owner name]
no rmon event index
```

Parameters

- **index**— Specifies the event index. (Range: 1–65535)
- **none**— Specifies that no notification is generated by the device for this event.
• **log**—Specifies that a notification entry is generated in the log table by the device for this event.

• **trap**—Specifies that an SNMP trap is sent to one or more management stations by the device for this event.

• **log-trap**—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.

• **community text**—Specifies the SNMP community (password) used when an SNMP trap is sent. (Octet string; length: 0–127 characters)

• **description text**—Specifies a comment describing this event. (Length: 0–127 characters)

• **owner name**—Specifies the name of the person who configured this event. (Valid string)

**Default Configuration**

If the owner name is not specified, it defaults to an empty string.

**Command Mode**

Global Configuration mode

**Example**

The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
switchxxxxxx(config)# rmon event 10 log
```

### 21.9 show rmon events

Use the **show rmon events** EXEC mode command to display the RMON event table.

**Syntax**

```
show rmon events
```

Command Mode
EXEC mode

Example
The following example displays the RMON event table.

```
switchxxxxxx# show rmon events
Index  Description  Type  Community  Owner  Last time sent
-----  -----------  ----  --------  ------  ------------------
 1      Errors      Log   router    CLI    Jan 18 2006 23:58:17
 2      High        Log   Manager   Jan 18 2006 23:59:48

Broadcast  Trap
```

The following table describes significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Unique index that identifies this event.</td>
</tr>
<tr>
<td>Description</td>
<td>Comment describing this event.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of notification that the device generates about this event. Can have</td>
</tr>
<tr>
<td></td>
<td>the following values: none, log, trap, log-trap. In the case of log, an</td>
</tr>
<tr>
<td></td>
<td>entry is made in the log table for each event. In the case of trap, an</td>
</tr>
<tr>
<td></td>
<td>SNMP trap is sent to one or more management stations.</td>
</tr>
<tr>
<td>Community</td>
<td>If an SNMP trap is to be sent, it is sent with the SNMP community string</td>
</tr>
<tr>
<td></td>
<td>specified by this octet string.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this event.</td>
</tr>
<tr>
<td>Last time sent</td>
<td>The time this entry last generated an event. If this entry has not</td>
</tr>
<tr>
<td></td>
<td>generated any events, this value is zero.</td>
</tr>
</tbody>
</table>

21.10  show rmon log
Use the `show rmon log` EXEC mode command to display the RMON log table.

Syntax
```
show rmon log [event]
```
Remote Network Monitoring (RMON) Commands

Parameters

**event**—Specifies the event index. (Range: 0–65535)

Command Mode

EXEC mode

Example

The following example displays event 1 in the RMON log table.

```
switchxxxxxx# show rmon log 1
Maximum table size: 500 (800 after reset)
Event Description Time
---- -------------- ---------
1 MIB Var.: 1.3.6.1.2.1.2.2.1.10.53, Delta, Rising, Actual Val: 800, Thres.Set: 100, Interval (sec): 1

Jan 18 2006 23:48:19
```

21.11 **rmon table-size**

Use the **rmon table-size** Global Configuration mode command to configure the maximum size of RMON tables. Use the no form of this command to return to the default size.

Syntax

```
rmon table-size {history entries | log entries}
no rmon table-size {history | log}
```

Parameters

- **history entries**—Specifies the maximum number of history table entries. (Range: 20–270)
- **log entries**—Specifies the maximum number of log table entries. (Range: 20–100)
Default Configuration
The default history table size is 270 entries.
The default log table size is 200 entries.

Command Mode
Global Configuration mode

User Guidelines
The configured table size takes effect after the device is rebooted.

Example
The following example configures the maximum size of RMON history tables to 100 entries.

switchxxxxxx(config)# rmon table-size history 100
22.1 aaa authentication dot1x

Use the **aaa authentication dot1x** Global Configuration mode command to specify how ports are authenticated when 802.1X is enabled. You can select either authentication by a RADIUS server, no authentication, or both methods. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
aaa authentication dot1x default method1 [method2]
no aaa authentication dot1x default
```

**Parameters**

- **method1 [method2]**—Specify at least one method from the following:
  - **radius** - Uses the list of all RADIUS servers for authentication
  - **none** - Uses no authentication

**Default Configuration**

The default method is RADIUS.

**Command Mode**

Global Configuration mode

**User Guidelines**

You can select either authentication by a RADIUS server, no authentication (**none**), or both methods.

If you require that authentication succeeds even if the RADIUS server is not found or returns an error, specify **none** as the final method in the command line.
Example
The following example sets the 802.1X authentication mode to RADIUS server authentication. If no response is received, no authentication is performed.

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

### 22.2 dot1x system-auth-control

Use the `dot1x system-auth-control` Global Configuration mode command to enable 802.1X globally. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
dot1x system-auth-control
no dot1x system-auth-control
```

**Parameters**

N/A

**Default Configuration**

Disabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables 802.1X globally.

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

### 22.3 dot1x port-control

Use the `dot1x port-control` Interface Configuration (Ethernet) mode command to enable manual control of the port authorization state. Use the `no` form of this command to restore the default configuration.
Syntax

dot1x port-control \{auto / force-authorized / force-unauthorized\}[time-range time-range-name]

no dot1x port-control

Parameters

- **auto**—Enables 802.1X authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the device and the client.

- **force-authorized**—Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1X-based client authentication.

- **force-unauthorized**—Denies all access through this port by forcing it to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through this port.

- **time-range time-range-name**—Specifies a time range. When the Time Range is not in effect, the port state is Unauthorized. (Range: 1–32 characters)

Default Configuration

The port is in the force-authorized state.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1X edge ports (ports in auto state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The following example sets 802.1X authentication on gi15 to auto mode.
22.4 dot1x reauthentication

Use the `dot1x reauthentication` Interface Configuration mode command to enable periodic re-authentication of the client. Use the `no` form of this command to return to the default setting.

Syntax

dot1x reauthentication

no dot1x reauthentication

Parameters

N/A

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface configuration (Ethernet)

Example

switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x reauthentication

22.5 dot1x timeout reauth-period

Use the `dot1x timeout reauth-period` Interface Configuration mode command to set the number of seconds between re-authentication attempts. Use the `no` form of this command to return to the default setting.

Syntax

dot1x timeout reauth-period `seconds`

no dot1x timeout reauth-period
Parameters

reauth-period seconds—Number of seconds between re-authentication attempts. (Range: 300-4294967295)

Default Configuration

3600

Command Mode

Interface Configuration (Ethernet) mode

Example

switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000

22.6  dot1x re-authenticate

The dot1x re-authenticate Privileged EXEC mode command manually initiates re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

Syntax

dot1x re-authenticate [interface-id]

Parameters

interface-id—Specifies an Ethernet port ID.

Default Configuration

If no port is specified, command is applied to all ports.

Command Mode

Privileged EXEC mode
Example
The following command manually initiates re-authentication of 802.1X-enabled gi15.

```
switchxxxxxx# dot1x re-authenticate gi15
```

### 22.7 dot1x timeout quiet-period

Use the `dot1x timeout quiet-period` Interface Configuration (Ethernet) mode command to set the time interval that the device remains in a quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the `no` form of this command to restore the default configuration.

**Syntax**

```
dot1x timeout quiet-period seconds
```

```
no dot1x timeout quiet-period
```

**Parameters**

`seconds`—Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with the client. (Range: 0–65535 seconds)

**Default Configuration**

The default quiet period is 60 seconds.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

During the quiet period, the device does not accept or initiate 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 that the device remains in the quiet state following a failed authentication exchange to 10 seconds.

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

22.8 dot1x timeout tx-period
Use the `dot1x timeout tx-period` Interface Configuration (Ethernet) mode command 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 `no` form of this command to restore the default configuration.

Syntax

```
dot1x timeout tx-period seconds
no dot1x timeout tx-period
```

Parameters

`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 (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 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 gi15
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

22.9 **dot1x max-req**

Use the `dot1x max-req` Interface Configuration mode command to set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
dot1x max-req count
no dot1x max-req
```

**Parameters**

- `max-req count`—Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10)

**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 times that the device sends an EAP request/identity frame to 6

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

### 22.10 dot1x timeout supp-timeout

Use the **dot1x timeout supp-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
dot1x timeout supp-timeout seconds
no dot1x timeout supp-timeout
```

**Parameters**

- `supp-timeout seconds`—Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 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 during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

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

### 22.11 dot1x timeout server-timeout

Use the `dot1x timeout server-timeout` Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response from the authentication server. Use the `no` form of this command to restore the default configuration.

**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 (Ethernet) 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 gi15
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

22.12 show dot1x

Use the `show dot1x` Privileged EXEC mode command to display the 802.1X
interfaces or specified interface status.

Syntax

```
show dot1x [interface interface-id | detailed]
```

Parameters

- `interface-id`—Specify an Ethernet port ID.
- `detailed`—Displays information for non-present ports in addition to present
  ports.

Default Configuration

Display for all ports. If `detailed` is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode
Examples

Example 1 - The following example displays the status of a single 802.1X-enabled Ethernet ports.

```
switchxxxxxx# show dot1x interface gi3
802.1X is enabled.
Port Admin Oper Reauth Reauth Username
Mode Mode Control Period
---- ----------- ---------- ------ ------ ------
gi3 Auto Unauthorized Ena 3600 Clark

Time-range: work-hours (Inactive now)
Quiet period: 60 Seconds
Tx period: 30 Seconds
Max req: 2
Supplicant timeout: 30 Seconds
Server timeout: 30 Seconds
Session Time (HH:MM:SS): 08:19:17
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Termination Cause: Supplicant logoff
Authenticator State Machine
State: HELD
Backend State Machine
State: IDLE
Authentication success: 9
Authentication fails: 1
```

Example 2 - The following example displays the status of all 802.1X-enabled Ethernet ports.

```
switchxxxxxx# show dot1x
802.1X is enabled
```
The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Admin mode</td>
<td>The port administration (configured) mode. Possible values: Force-auth, Force-unauth, Auto.</td>
</tr>
<tr>
<td>Oper mode</td>
<td>The port operational (actual) mode. Possible values: Authorized, Unauthorized or Down.</td>
</tr>
<tr>
<td>Reauth Control</td>
<td>Reauthentication control.</td>
</tr>
<tr>
<td>Reauth Period</td>
<td>Reauthentication period.</td>
</tr>
<tr>
<td>Username</td>
<td>Username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authenticated successfully.</td>
</tr>
<tr>
<td>Quiet period</td>
<td>Number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).</td>
</tr>
<tr>
<td>Tx period</td>
<td>Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request.</td>
</tr>
<tr>
<td>Max req</td>
<td>Maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.</td>
</tr>
<tr>
<td>Supplicant timeout</td>
<td>Number of seconds that the device waits for a response to an EAP-request frame from the client before resending the request.</td>
</tr>
</tbody>
</table>
22.13 show dot1x users

Use the `show dot1x users` Privileged EXEC mode command to display active 802.1X authenticated users for the device.

**Syntax**

```
show dot1x users [username username]
```

**Parameters**

- **username**—Specifies the supplicant username (Length: 1–160 characters)

**Default Configuration**

Display all users.

**Command Mode**

Privileged EXEC mode
Example

The following example displays 802.1X user with supplicant username Bob.

```
switchxxxxxx# show dot1x users username Bob
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>Session</th>
<th>Auth</th>
<th>MAC</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Bob</td>
<td>1d 09:07:38</td>
<td>Remote</td>
<td>0008.3b79.8787</td>
<td>3</td>
</tr>
</tbody>
</table>

22.14 show dot1x statistics

Use the `show dot1x statistics` Privileged EXEC mode command to display 802.1X statistics for the specified port.

Syntax

```
show dot1x statistics interface interface-id
```

Parameters

`interface-id`—Specifies an Ethernet port ID.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1X statistics for `gi1`.

```
switchxxxxxx# show dot1x statistics interface gi1
EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
```
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EapolFramesRx</td>
<td>Number of valid EAPOL frames of any type that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolFramesTx</td>
<td>Number of EAPOL frames of any type that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EapolStartFramesRx</td>
<td>Number of EAPOL Start frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolLogoffFramesRx</td>
<td>Number of EAPOL Logoff frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespldFramesRx</td>
<td>Number of EAP Resp/Id frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespFramesRx</td>
<td>Number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqIdFramesTx</td>
<td>Number of EAP Req/Id frames that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqFramesTx</td>
<td>Number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>InvalidEapolFramesRx</td>
<td>Number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.</td>
</tr>
</tbody>
</table>
22.15 clear dot1x statistics

Use the `clear dot1x statistics` Privileged EXEC mode command to clear 802.1X statistics.

**Syntax**

```
clear dot1x statistics [interface-id]
```

**Parameters**

- `interface-id`—Specify an Ethernet port ID.

**Default Configuration**

Statistics on all ports are cleared.

**Command Mode**

Privileged EXEC

**User Guidelines**

The command clears the statistics displayed in the `show dot1x statistics` command.

**Example**

```
switchxxxxxx# clear dot1x statistics
```
22.16 dot1x host-mode

Use the dot1x host-mode Interface Configuration mode command to allow a single host (client) or multiple hosts on an IEEE 802.1X-authorized port. Use the no form of this command to return to the default setting.

Syntax

dot1x host-mode \{multi-host / single-host / multi-sessions\}

Parameters

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

Default Configuration

Default mode is multi-host.

Command Mode

Interface Configuration (Ethernet) 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.

Port security on a port cannot be enabled in single-host mode and in multiple-sessions mode.

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

switchxxxxx(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

### 22.17 dot1x auth-not-req

Use the `dot1x auth-not-req` Interface Configuration (VLAN) mode command to enable unauthorized devices access to the VLAN. Use the `no` form of this command to disable access to the VLAN.

**Syntax**

dot1x auth-not-req

no dot1x auth-not-req

**Parameters**

N/A

**Default Configuration**

Access is enabled.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets are accepted in the unauthorized state).

**Example**

The following example enables unauthorized devices access to VLAN 5.

switchxxxxxx(config)# interface vlan 5
switchxxxxxx(config-if)# dot1x auth-not-req
22.18  **dot1x violation-mode**

Use the `dot1x violation-mode` Interface Configuration (Ethernet) mode command 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 `no` form of this command to return to default.

**Syntax**

```
dot1x violation-mode {restrict / protect / shutdown}[traps 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 address 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
- **traps seconds** - Send SNMP traps, and specifies the minimum time between consecutive traps. If seconds = 0 traps are disabled. If the parameter is not specified it defaults to 1 second for the restrict mode and 0 for the other modes.

**Default Configuration**

Protect

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

The command is relevant only for single-host mode.

BPDU message whose MAC address is not the supplicant MAC address wouldn't be discarded in the protect mode.

BPDU message whose MAC address is not the supplicant MAC address would cause a shutdown in the shutdown mode.
### Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x violation-mode protect
```

#### 22.19 dot1x guest-vlan

Use the **dot1x guest-vlan** Interface Configuration (VLAN) mode command to define a guest VLAN. Use the **no** form of this command to restore the default configuration.

**Syntax**

```
dot1x guest-vlan
no dot1x guest-vlan
```

**Parameters**

N/A

**Default Configuration**

No VLAN is defined as a guest VLAN.

**Command Mode**

Interface Configuration (VLAN) 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 port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

**Example**

The following example defines VLAN 2 as a guest VLAN.

```
switchxxxxxx(config)# interface vlan 2
```
22.20  dot1x guest-vlan timeout

Use the dot1x guest-vlan timeout Global Configuration mode command to set the
time delay between enabling 802.1X (or port up) and adding a port to the guest
VLAN. Use the no form of this command to restore the default configuration.

Syntax

    dot1x guest-vlan timeout timeout

    no dot1x guest-vlan timeout

Parameters

    timeout—Specifies the time delay in seconds between enabling 802.1X (or port
    up) and adding the port to the guest VLAN. (Range: 30–180)

Default Configuration

    The guest VLAN is applied immediately.

Command Mode

    Global Configuration mode

User Guidelines

    This command is relevant if the guest VLAN is enabled on the port. Configuring the
timeout adds delay from enabling 802.1X (or port up) to the time the device adds
the port to the guest VLAN.

Example

    The following example sets the delay between enabling 802.1X and adding a port
to a guest VLAN to 60 seconds.

    switchxxxxxx(config)# dot1x guest-vlan timeout 60
### 22.21 dot1x guest-vlan enable

Use the `dot1x guest-vlan enable` Interface Configuration (Ethernet) mode command to enable unauthorized users on the interface access to the guest VLAN. Use the `no` form of this command to disable access.

**Syntax**

- `dot1x guest-vlan enable`
- `no dot1x guest-vlan enable`

**Parameters**

N/A

**Default Configuration**

The default configuration is disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

A device can have only one global guest VLAN. The guest VLAN is defined using the `dot1x guest-vlan` Interface Configuration mode command.

**Example**

The following example enables unauthorized users on `gi 1` to access the guest VLAN.

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

### 22.22 dot1x mac-authentication

Use the `dot1x mac-authentication` Interface Configuration (Ethernet) mode command to enable authentication based on the station’s MAC address. Use the `no` form of this command to disable this feature.
802.1X Commands

Syntax

dot1x mac-authentication \{mac-only\ | mac-and-802.1x\}

no dot1x mac-authentication

Parameters

- **mac-only**—Enables authentication based on the station's MAC address only. 802.1X frames are ignored.
- **mac-and-802.1x**—Enables 802.1X authentication and MAC address authentication on the interface.

Default Configuration

Authentication based on the station's MAC address is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The guest VLAN must be enabled when MAC authentication is enabled.

Static MAC addresses cannot be authorized. Do not change an authenticated MAC address to a static address.

It is not recommended to delete authenticated MAC addresses.

Reauthentication must be enabled when working in this mode.

Example

The following example enables authentication based on the station's MAC address on gi1.

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# dot1x mac-authentication mac-only
```

22.23 dot1x radius-attributes vlan

Use the **dot1x radius-attributes vlan** Interface Configuration mode command to enable user-based VLAN assignment.
Use the **no** form of this command to disable user-based VLAN assignment.

**Syntax**

```plaintext
dot1x radius-attributes vlan [reject | vlan-id]
nodot1x radius-attributes vlan
```

**Parameters**

- **reject**—If the RADIUS server authenticated the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected. If the parameter is omitted, this option is applied by default.

- **vlan-id**—If the RADIUS server authenticated the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted, and the configured VLAN is assigned to the supplicant.

**Default Configuration**

Disabled

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

The configuration of this command is allowed only when the port is Forced Authorized.

RADIUS attributes are supported only in Multiple Sessions mode (multiple hosts with authentication)

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

Packets to the supplicant are sent untagged.

After successful authentication, the port remains a member in the unauthenticated VLANs and in the guest VLAN. Other static VLAN configurations are not applied on the port.
Example

Example 1—The example enables user-based VLAN assignment. If the RADIUS server authenticated the supplicant but did not provide a supplicant VLAN, the supplicant is rejected.

```
switchxxxxxx(config)# interface 151
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

Example 2—The example enables user-based VLAN assignment. If the RADIUS server authenticated the supplicant but did not provide a supplicant VLAN the supplicant is accepted and VLAN 100 is assigned to the supplicant.

```
switchxxxxxx(config)# interface 151
switchxxxxxx(config-if)# dot1x radius-attributes vlan 100
switchxxxxxx(config-if)# exit
```

22.24 show dot1x advanced

Use the `show dot1x advanced` Privileged EXEC mode command to display 802.1x advanced features for the device or specified interface.

Syntax

```
show dot1x advanced [interface-id | detailed]
```

Parameters

- `interface-id`—Specify an Ethernet port ID.
- `detailed`—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If the `detailed` parameter is not used, only present ports are displayed.
Command Mode

Privileged EXEC mode

Examples

The following example displays the 802.1x advanced features for the device. Notice that port 3 has a user-defined alternative VLAN (1023).

```
switchxxxxxx# show dot1x advanced
Guest VLAN: 3978
Guest VLAN Timeout:
Unauthenticated VLANs: 91, 92

Interface Multiple Guest MAC VLAN
Hosts VLAN Authentication Assignment
------- ---------- ------ ---------------- -----------
151 Disabled Enabled MAC-and-802.1X Enabled
152 Enabled Disabled Disabled Enabled
153 Disabled Enabled MAC-and-802.1X Enabled

switchxxxxxx# show dot1x advanced 151

Interface Multiple Guest MAC VLAN
Hosts VLAN Authentication Assignment
------------------ -----------------------  -----------
151 Disabled Enabled MAC-and-802.1X Enabled

Legacy-Supp mode is disabled
Policy assignment resource err handling: Accept
Single host parameters
Violation action: Discard
Trap: Enabled
Status: Single-host locked
Violations since last trap: 9
```
23.1 interface

Use the interface Global Configuration mode command to enter Interface configuration mode in order to configure an interface.

Syntax

interface interface-id

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel, VLAN, range, IP interface or tunnel.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, Port-channel, VLAN, range, IP interface or tunnel) mode

Examples

Example 1 - For Gigabit Ethernet ports:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)#
```

Example 3 - For port channels (LAGs):

```
switchxxxxxx(config)# interface po1
switchxxxxxx(config-if)#
```
23.2 interface range

Use the interface range command to execute a command on multiple ports at the same time.

Syntax

interface range interface-id-list

Parameters

interface-id-list—Specify list of interface IDs. The interface ID can be one of the following types: Ethernet port, VLAN, or Port-channel

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, Port-channel, or VLAN) mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range: If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Example

switchxxxxxx(config)# interface range gi1-20
switchxxxxxx(config-if-range)#

23.3 shutdown

Use the shutdown Interface Configuration (Ethernet, Port-channel) mode command to disable an interface. Use the no form of this command to restart a disabled interface.

Syntax

shutdown

no shutdown
Parameters
N/A

Default Configuration
The interface is enabled.

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

Examples
Example 1 - The following example disables gi5 operations.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 2 - The following example restarts the disabled Ethernet port.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# no shutdown
switchxxxxxx(config-if)
```

23.4 operation time

Use the operation time Interface Configuration (Ethernet) mode command to control the time that the port is up. Use the no form of this command to cancel the time range for the port operation time.

Syntax

```
operation time time-range-name
no operation time
```
Parameters

- **time-range-name**—Specifies a time range the port operates (in up state). When the Time Range is not in effect, the port is shutdown. (Range: 1–32 characters)

Default Configuration

There is no time range configured on the port authorized state.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in auto state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The operation time command influences the port if the port status is up. This command defines the time frame during which the port stays up and at which time the port will be shutdown. While the port is in shutdown because of other reasons, this command has no effect.

The following example activates an operation time range (named "morning") on gigabitethernet port 1/1/15.

```plaintext
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# operation time morning
```

23.5 **description**

Use the **description** Interface Configuration (Ethernet, Port-channel) mode command to add a description to an interface. Use the **no** form of this command to remove the description.

Syntax

```plaintext
description string
```

```plaintext
no description
```
Parameters

string—Specifies a comment or a description of the port to assist the user. (Length: 1–64 characters).

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example adds the description ‘SW#3’ to gi5.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# description SW#3
```

23.6 speed

Use the `speed` Interface Configuration (Ethernet, Port-channel) mode command to configure the speed of a given Ethernet interface when not using auto-negotiation. Use the `no` form of this command to restore the default configuration.

Syntax

```
speed {10 | 100 | 1000 | 10000}
no speed
```

Parameters

- 10—Forces 10 Mbps operation.
- 100—Forces 100 Mbps operation.
- 1000—Forces 1000 Mbps operation.

Default Configuration

The port operates at its maximum speed capability.
**Command Mode**

Interface Configuration (Ethemet, Port-channel) mode

**User Guidelines**

The `no speed` command in a port-channel context returns each port in the port-channel to its maximum capability.

**Example**

The following example configures the speed of gi5 to 100 Mbps operation.

```
switchxxxxx(config)# interface gi5
switchxxxxx(config-if)# speed 100
```

## 23.7 `duplex`

Use the `duplex` Interface Configuration (Ethernet, Port-channel) mode command to configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
duplex {half | full}
no duplex
```

**Parameters**

- `half`—Forces half-duplex operation.
- `full`—Forces full-duplex operation.

**Default Configuration**

The interface operates in full duplex mode.

**Command Mode**

Interface Configuration (Port-channel) mode
Example
The following example configures gi5 to operate in full duplex mode.

```
switchxxxxx(config)# interface gi5
switchxxxxx(config-if)# duplex full
```

## 23.8 negotiation

Use the `negotiation` Interface Configuration (Ethernet, Port-channel) mode command to enable auto-negotiation operation for the speed and duplex parameters and master-slave mode of a given interface. Use the `no` form of this command to disable auto-negotiation.

**Syntax**

```
negotiation [capability [capability2... capability5]] [preferred {master | slave}]
negotiation
no negotiation
```

**Parameters**

- **Capability**—Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h, 100f, 1000f).
  - 10h - Advertise 10 half-duplex
  - 10f - Advertise 10 full-duplex
  - 100h - Advertise 100 half-duplex
  - 100f - Advertise 100 full-duplex
  - 1000f - Advertise 1000 full-duplex
- **Preferred** - Specifies the master-slave preference:
  - Master - Advertise master preference
  - Slave - Advertise slave preference

**Default Configuration**

If capability is unspecified, defaults to list of all the capabilities of the port and preferred master mode.
Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example enables auto-negotiation on gi5.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# negotiation
```

### 23.9 flowcontrol

Use the `flowcontrol` Interface Configuration (Ethernet, Port-channel) mode command to configure the Flow Control on a given interface. Use the `no` form of this command to disable Flow Control.

**Syntax**

```
flowcontrol {auto | on | off}
no flowcontrol
```

**Parameters**

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

**Default Configuration**

Flow control is disabled.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

Use the `negotiation` command to enable `flow control auto`. 
Example

The following example enables Flow Control on port gi1

```plaintext
switchxxxxx(config)# interface gi1
switchxxxxx(config-if)# flowcontrol on
```

23.10 mdix

Use the `mdix` Interface Configuration (Ethernet) mode command to enable cable crossover on a given interface. Use the `no` form of this command to disable cable crossover.

Syntax

```plaintext
mdix {on | auto}
no mdix
```

Parameters

- **on**—Enables manual MDIX.
- **auto**—Enables automatic MDI/MDIX.

Default Configuration

The default setting is On.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables automatic crossover on port gi5.

```plaintext
switchxxxxx(config)# interface gi5
switchxxxxx(config-if)# mdix auto
```
23.11  **back-pressure**

Use the **back-pressure** Interface Configuration (Ethernet) mode command to enable back pressure on a specific interface. Use the **no** form of this command to disable back pressure.

**Syntax**

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

**Default Configuration**

Back pressure is disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

Back-pressure cannot be enabled when EEE is enabled.

**Example**

The following example enables back pressure on port gi5.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# back-pressure
```

23.12  **port jumbo-frame**

Use the **port jumbo-frame** Global Configuration mode command to enable jumbo frames on the device. Use the **no** form of this command to disable jumbo frames.

**Syntax**

```
port jumbo-frame
no port jumbo-frame
```
Default Configuration
Jumbo frames are disabled on the device.

Command Mode
Global Configuration mode

User Guidelines
This command takes effect only after resetting the device.

Example
The following example enables jumbo frames on the device.

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

23.13 clear counters
Use the clear counters EXEC mode command to clear counters on all or on a specific interface.

Syntax
```
clear counters [interface-id]
```

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
All counters are cleared.

Command Mode
EXEC mode

Example
The following example clears the statistics counters for gi5.

```
```
23.14  **set interface active**

Use the **set interface active** EXEC mode command to reactivate an interface that was shut down.

**Syntax**

```
set interface active [interface-id]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode

**User Guidelines**

This command is used to activate interfaces that were configured to be active, but were shut down by the system.

**Example**

The following example reactivates **gi1**

```
switchxxxxxx# set interface active gi1
```

23.15  **show interfaces configuration**

Use the **show interfaces configuration** EXEC mode command to display the configuration for all configured interfaces or for a specific interface.

**Syntax**

```
show interfaces configuration [interface-id [detailed]]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays the configuration of all configured interfaces:

```
switchxxxxxx# show interfaces configuration
```

<table>
<thead>
<tr>
<th>Flow</th>
<th>Admin</th>
<th>Back</th>
<th>Mdix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Type</td>
<td>Duplex</td>
<td>Speed</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>gi1</td>
<td>1G-Copper</td>
<td>Full</td>
<td>10000</td>
</tr>
<tr>
<td>gi2</td>
<td>1G-Copper</td>
<td>Full</td>
<td>1000</td>
</tr>
</tbody>
</table>

```

```
 Flow Admin
 PO Type Speed Neg Control State
 ------ ------ ---- ------- ------ ---- |
 Po1 Disabled Off Up

```

**23.16 show interfaces status**

Use the `show interfaces status` EXEC mode command to display the status of all interfaces or of a specific interface.

**Syntax**

```
show interfaces status [interface-id | detailed]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Command Mode**

EXEC mode

**Default Configuration**

Display for all interfaces. If detailed is not used, only present ports are displayed.

**Example**

The following example displays the status of all configured interfaces.

```
switchxxxxxx# show interfaces status

Flow  Link   Back     Mdix
Port  Type      Duplex Speed Neg      ctrl  State  Pressure Mode
------ --------- ------ ----- -------- ----  ------ -------- --
gi1   1G-Copper Full   1000  Disabled Off   Up     Disabled Off

gi2   1G-Copper --     --     --      --    Down   --       --

Flow  Link
PO    Type      Duplex Speed  Neg     control  State
-----  -------   ------ -----  ------- ----     ----
Po1    1G        Full   10000  Disabled Off     Up
```

**23.17 show interfaces advertise**

Use the `show interfaces advertise` EXEC mode command to display auto-negotiation advertisement information for all configured interfaces or for a specific interface.

**Syntax**

```
show interfaces advertise [interface-id [detailed]]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**Examples**

The following examples display auto-negotiation information.

```
switchxxxxxx# show interfaces advertise
  Port  Type        Neg  Preferred  Operational Link Advertisement
  ----  --------    ----  ---------  ---------------------------
  gi1   1G-Copper   Enable  Master              1000f, 100f, 10f, 10h
  gi2   1G-Copper   Enable  Slave

switchxxxxxx# show interfaces advertise gi1
  Port: gi1
  Type: 1G-Copper
  Link state: Up
  Auto Negotiation: enabled
  Preference: Master

  10h  10f  100h  100f
  ---  ---  ----  ----
  Admin Local link Advertisement                    yes  yes  yes
  Oper Local link Advertisement                     yes  yes  yes  ---  yes
  Remote Local link Advertisement                   no  no  yes  yes  yes
  Priority Resolution                                yes

switchxxxxxx# show interfaces advertise gi1
  Port: gi1
  Type: 1G-Copper
  Link state: Up
  Auto negotiation: disabled.
  Preference: Slave
```
23.18  show interfaces description

Use the **show interfaces description** EXEC mode command to display the description for all configured interfaces or for a specific interface.

**Syntax**

```
show interfaces description [interface-id | detailed]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display description for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays the description of all configured interfaces.

```
switchxxxxxx# show interfaces description
Port   Descriptions
gi1    -------------------------------------------------------------
gi2    Port that should be used for management only
gi3
gi4
PO    Description
----   --------
Po1    Output
```
### 23.19 show interfaces counters

Use the `show interfaces counters` EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

#### Syntax

```
show interfaces counters [interface-id | detailed]
```

#### Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

#### Default Configuration

Display counters for all interfaces. If `detailed` is not used, only present ports are displayed.

#### Command Mode

EXEC mode

#### Example

The following example displays traffic seen by all the physical interfaces.

```
switchxxxxxx# show interfaces counters gi1
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
  gi1           0            0            0            0

Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
  gi1           0            1            35          7051
```

Alignment Errors: 0

FCS Errors: 0

Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
The following table describes the fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>Number of received octets.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>Number of received unicast packets.</td>
</tr>
<tr>
<td>InMcastPkts</td>
<td>Number of received multicast packets.</td>
</tr>
<tr>
<td>InBcastPkts</td>
<td>Number of received broadcast packets.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Number of transmitted octets.</td>
</tr>
<tr>
<td>OutUcastPkts</td>
<td>Number of transmitted unicast packets.</td>
</tr>
<tr>
<td>OutMcastPkts</td>
<td>Number of transmitted multicast packets.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>Number of transmitted broadcast packets.</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>Number of frames received that are an integral number of octets in length but do not pass the FCS check.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>Number of frames that are involved in a single collision, and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>Number of frames that are involved in more than one collision and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>SQE Test Errors</td>
<td>Number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.</td>
</tr>
<tr>
<td>Deferred Transmissions</td>
<td>Number of frames for which the first transmission attempt is delayed because the medium is busy.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>Number of times that a collision is detected later than one slotTime into the transmission of a packet.</td>
</tr>
<tr>
<td>Excessive Collisions</td>
<td>Number of frames for which transmission fails due to excessive collisions.</td>
</tr>
<tr>
<td>Oversize Packets</td>
<td>Number of frames received that exceed the maximum permitted frame size.</td>
</tr>
<tr>
<td>Internal MAC Rx Errors</td>
<td>Number of frames for which reception fails due to an internal MAC sublayer receive error.</td>
</tr>
</tbody>
</table>
23.20 show ports jumbo-frame

Use the show ports jumbo-frame EXEC mode command to display the whether jumbo frames are enabled on the device.

Syntax

show ports jumbo-frame

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays whether jumbo frames are enabled on the device.

```
switchxxxxxx# show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```
23.21 show errdisable interfaces

Use the show errdisable interfaces EXEC mode command to display the Err-Disable state of all interfaces or of a specific interface.

Syntax

show errdisable interfaces [interface-id]

Parameters

- interface—Interface number
- port-channel-number—Port channel index.

Default Configuration

Display for all interfaces.

Command Mode

EXEC mode

Example

The following example displays the Err-Disable state of all interfaces.

switchxxxxxx# show errdisable interfaces
Interface Reason
---------- ---------------
gi20 stp-bpdu-guard

23.22 storm-control broadcast enable

Use the storm-control broadcast enable Interface Configuration mode command to enable storm control on a port. Use the no form of this command to disable storm control.

Syntax

storm-control broadcast enable
no storm-control broadcast enable
Parameters
This command has no arguments or keywords.

Default Configuration
Disabled

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Use the `storm-control include-multicast` Interface Configuration command to count Multicast packets and optionally unknown Unicast packets in the storm control calculation.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# storm-control broadcast enable
```

### 23.23 storm-control broadcast level

Use the `storm-control broadcast level` Interface Configuration mode command to configure the maximum rate of broadcast. Use the `no` form of this command to return to default.

**Syntax**

```
storm-control broadcast level {level | kbps kbps}
```

**Parameters**

- **level**—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1 -100)
- **kbps**—Maximum of kilobits per second of broadcast traffic on a port. (Range 70–10000000)
Default Configuration

- **level**—10%
- **kbps**—10% of port speed in Kbps

Command Mode

Interface Configuration mode (Ethernet)

User Guidelines

Use the `storm-control broadcast enable` Interface Configuration command to enable storm control.

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 50 kbps 12345
```

23.24 storm-control include-multicast

Use the `storm-control include-multicast` Interface Configuration mode command to count Multicast packets in a Broadcast storm control. Use the `no` form of this command to disable counting of Multicast packets in the Broadcast storm control.

Syntax

```
storm-control include-multicast [unknown-unicast]
no storm-control include-multicast
```

Parameters

- **unknown-unicast**—Specifies also the count of unknown unicast packets.

Default Configuration

Disabled

Command Mode

Interface Configuration mode (Ethernet)
23.25  show storm-control

Use the show storm-control EXEC mode command to display the configuration of storm control for a port.

Syntax

show storm-control [interface-id]

Parameters

interface-id—Specifies the Ethernet port.

Default Configuration

Display for all interfaces.

Command Mode

EXEC mode

Example

switchxxxxxx# show storm-control

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Admin Rate [Kb/Sec]</th>
<th>Oper Rate [Kb/Sec]</th>
<th>Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>12345</td>
<td>12345</td>
<td>Broadcast, Multicast, Unknown Unicast</td>
</tr>
<tr>
<td>gi2</td>
<td>Disabled</td>
<td>100000</td>
<td>100000</td>
<td>Broadcast</td>
</tr>
<tr>
<td>gi3</td>
<td>Enabled</td>
<td>10%</td>
<td>000000</td>
<td>Broadcast</td>
</tr>
</tbody>
</table>
24.1 test cable-diagnostics tdr

Use the test cable-diagnostics tdr Privileged EXEC mode command to use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test cable-diagnostics tdr interface interface-id

Parameters

interface-id—Specifies an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The port to be tested should be shut down during the test, unless it is a combination port with fiber port active.

The maximum length of cable for the TDR test is 120 meters.

Example

The following examples test the copper cables attached to ports 7 and 8.

```
switchxxxxxx# test cable-diagnostics tdr interface gi7
Cable is open at 64 meters
switchxxxxxx# test cable-diagnostics tdr interface gi8
Can't perform the test on fiber ports
```
24.2 show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** EXEC mode command to display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port.

**Syntax**

```
show cable-diagnostics tdr [interface interface-id | detailed]
```

**Parameters**

- **interface-id**—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

All ports are displayed. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**User Guidelines**

The maximum length of cable for the TDR test is 120 meters.

**Example**

The following example displays information on the last TDR test performed on all copper ports.

```
switchxxxxxx# show cable-diagnostics tdr
Port Result Length Date
---- ------ [meters] --------------
       ----
gi1  OK

Port Result Length Date
---- ------ [meters] --------------
       ----
gi2  Short 50 13:32:00 23 July 2010

Port Result Length Date
---- ------ [meters] --------------
       ----
gi3  Test has not been performed

Port Result Length Date
---- ------ [meters] --------------
       ----
gi4  Open 64 13:32:00 23 July 2010

Port Result Length Date
---- ------ [meters] --------------
       ----
gi5  Fiber - -
```
24.3  show cable-diagnostics cable-length

Use the show cable-diagnostics cable-length EXEC mode command to display the estimated copper cable length attached to all ports or to a specific port.

Syntax

show cable-diagnostics cable-length [interface interface-id | detailed]

Parameters

- **interface-id**—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

User Guidelines

The port must be active and working at 100 M or 1000 M.

Example

The following example displays the estimated copper cable length attached to all ports.

```
switchxxxxxx# show cable-diagnostics cable-length
Port         Length [meters]
------------- -----------------
   gi1        < 50
   gi2    Copper not active
   gi3        110-140
   gi4            Fiber
```
24.4 show fiber-ports optical-transceiver

Use the show fiber-ports optical-transceiver EXEC mode command to display the optical transceiver diagnostics.

Syntax

```
show fiber-ports optical-transceiver [interface interface-id | detailed]
```

Parameters

- **interface-id**—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following examples display the optical transceiver diagnostics results.

```
switchxxxxxx# show fiber-ports optical-transceiver

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output</th>
<th>Input</th>
<th>LOS Power</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi1</td>
<td>W</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>gi2</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>E</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>

Temp - Internally measured transceiver temperature
Voltage - Internally measured supply voltage
Current - Measured TX bias current
Output Power - Measured TX output power 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

```
switchxxxxxx# show fiber-ports optical-transceiver

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output Power</th>
<th>Input Power</th>
<th>LOS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[C]</td>
<td>[Volt]</td>
<td>[mA]</td>
<td>Power [mWatt]</td>
<td>Power [mWatt]</td>
<td></td>
</tr>
<tr>
<td>gi1</td>
<td>28</td>
<td>3.32</td>
<td>7.26</td>
<td>3.53</td>
<td>3.68</td>
<td>No</td>
</tr>
<tr>
<td>gi6</td>
<td>29</td>
<td>3.33</td>
<td>6.50</td>
<td>3.53</td>
<td>3.71</td>
<td>No</td>
</tr>
</tbody>
</table>

Temp - Internally measured transceiver temperature  
Voltage - Internally measured supply voltage  
Current - Measured TX bias current  
Output Power - Measured TX output power 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
```
Power over Ethernet (PoE) Commands

25.1 power inline

Use the power inline Interface Configuration mode command to configure the power on an interface.

Syntax

```
power inline {auto / never} [time-range time-range-name]
```

Parameters

- **auto**—Turns on the device discovery protocol and applies power to the device.
- **never**—Turns off the device discovery protocol and stops applying power to the device.
- **auto time-range-name**—Turns on the power in the specified time range. When the time range is not in effect the power is not supplied to the attached device. If a time range is not specified, there is no time range bound to the port.
- **never time-range-name**—Turns off the power to the device in the specified time range. When the time range is not in effect the power is supplied to the attached device. If a time range is not specified, there is no time range bound to the port.

Default Configuration

The default configuration is set to **auto**.

Command Mode

Interface Configuration (Ethernet) mode

Usage Guidelines

The time range is defined in the **time-range** command.
Examples

Exercise 1—The following example turns on the inline power administrative mode on an interface.

```
switchxxxxxx(config)# interface 154
switchxxxxxx(config-if)# power inline auto
```

Exercise 2—The following example shows defining a time range called morning, and then applying it to the power administrative mode.

```
switchxxxxxx(config)#time-range morning
switchxxxxxx(config-time-range)#periodic list 07:00 to 11:59 mon wed fri
switchxxxxxx(config)#interface 151
switchxxxxxx(config-if)#power inline auto time-range morning
```

25.2 power inline powered-device

Use the `power inline powered-device` Interface Configuration mode command to add a description of the powered device type. Use the `no` form of this command to remove the description.

**Syntax**

```
power inline powered-device pd-type
no power inline powered-device
```

**Parameters**

`pd-type`—Enters a comment or a description to assist in recognizing the type of the powered device attached to this interface. (Length: 1–24 characters)

**Default Configuration**

There is no description.

**Command Mode**

Interface Configuration (Ethernet) mode
Example
The following example adds the description ‘ip phone’ of the device connected to port 4.

```
switchxxxxxx(config)# interface gi4
switchxxxxxx(config-if)# power inline powered-device ip_phone
```

### 25.3 power inline priority

Use the `power inline priority` Interface Configuration (Ethernet) mode command to configure the interface inline power management priority. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
power inline priority {critical | high | low}
```

**no power inline priority**

**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 configuration is set to low priority.

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example sets the inline power management priority of gigabitethernet port 4 to High.

```
switchxxxxxx(config)# interface gi4
switchxxxxxx(config-if)# power inline priority high
```
25.4  **power inline usage-threshold**

Use the `power inline usage-threshold` Global Configuration mode command to configure the threshold for initiating inline power usage alarms. Use the `no` form of this command to restore the default configuration.

**Syntax**

```plaintext
power inline usage-threshold percent
no power inline usage-threshold
```

**Parameters**

`percent`—Specifies the threshold in percent to compare to the measured power. (Range: 1–99)

**Default Configuration**

The default threshold is 95 percent.

**Command Mode**

Global Configuration mode

**Example**

The following example configures the threshold for initiating inline power usage alarms to 90 percent.

```
switchxxxxxx(config)# power inline usage-threshold 90
```

25.5  **power inline traps enable**

Use the `power inline traps enable` Global Configuration mode command to enable inline power traps. Use the `no` form of this command to disable traps.

**Syntax**

```plaintext
power inline traps enable
no power inline traps enable
```
Default Configuration

Inline power traps are disabled.

Command Mode

Global Configuration mode

Example

The following example enables inline power traps.

```
switchxxxxxx(config)# power inline traps enable
```

25.6 power inline limit

Use the `power inline limit` Interface Configuration mode command to configure the power limit per port on an interface. Use the `no` form of the command to return to default.

Syntax

```
power inline limit power
no power inline limit
```

Parameters

- `power`—States the port power consumption limit in Milliwatts (Range: The parameter range depends on the current working mode: In POE mode: 0-15400, In POE+ mode: 0–30000)

Default Configuration

The default value is the maximum power allowed in the specific working mode: 15.4W.

- In POE mode: 15.4W
- In POE+ mode: 30W

Command Mode

Interface Configuration (Ethernet) mode
25 Power over Ethernet (PoE) Commands

Example

The following example sets inline power on a port.

switchxxxxx(config)# interface gi1
switchxxxxx(config-if)# power inline limit 2222

25.7 power inline limit-mode

Use the `power inline limit-mode` Global Configuration mode command to set the power limit mode of the system. Use the `no` form of this command to return to default.

Syntax

```
power inline limit-mode {class | port}
no power inline limit-mode
```

Parameters

- **class**—The power limit of a port is based on the class of the PD (Power Device) as detected during the classification process
- **port**—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 sets the power limit to class.

```
switchxxxxx(config)# power inline limit-mode class
```

25.8 show power inline

Use the `show power inline` EXEC mode command to display information about the inline power for all interfaces or for a specific interface.
Syntax

`show power inline [interface-id | detailed]`

Parameters

- `interface-id`—Specifies an interface ID. The interface ID must be an Ethernet port.
- `detailed`—Displays information for non-present ports in addition to present ports.

Default Configuration

Show information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following example displays information about the inline power for all ports (port power based).

```
switchxxxxxx(config)# show power inline
Power limit: 15 W
Power limit (for port based power-limit mode): 15 W
Power Nominal Consumed Usage Traps
       Power       Power  Threshold
------- -------    -----------    ------     --------
       ----- ------    ----------    ------     
  1     Off  1 Watts  0 Watts (0%)  95      Disable

Port Powered Device State Status Priority Class
----- -------------- ------ ------ -------- ------ ------ ------ ------- ------
gi1 IP Phone Model A Auto  On     High    Class0

gi2 Wireless AP Model A Auto  On     Low    Class1

gi3                Auto  Off     Low    N/A
```
Example
The following example displays information about the inline power for a specific port.

```
switchxxxxxx(config)# show power inline gi1
Power limit: 15 W
Power limit (for port based power-limit mode): 15 W

Port   Powered Device        State      Status    Priority  Class
-----   --------------      -----------  --------  --------  -------
   gi1     IP Phone Model A     Auto         On       High      Class0
```

The following table describes the fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Inline power sourcing equipment operational status.</td>
</tr>
<tr>
<td>Nominal Power</td>
<td>Inline power sourcing equipment nominal power in Watts.</td>
</tr>
<tr>
<td>Consumed Power</td>
<td>Measured usage power in Watts.</td>
</tr>
<tr>
<td>Usage Threshold</td>
<td>Usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.</td>
</tr>
<tr>
<td>Traps</td>
<td>Indicates if inline power traps are enabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Ethernet port number.</td>
</tr>
<tr>
<td>Powered device</td>
<td>Description of the powered device type.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates if the port is enabled to provide power. The possible values are Auto or Never.</td>
</tr>
<tr>
<td>Priority</td>
<td>Port inline power management priority. The possible values are Critical, High or Low.</td>
</tr>
<tr>
<td>Status</td>
<td>Power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.</td>
</tr>
<tr>
<td>Class</td>
<td>Power consumption classification of the powered device.</td>
</tr>
<tr>
<td>Overload Counter</td>
<td>Counts the number of overload conditions detected.</td>
</tr>
</tbody>
</table>
Following is a list of port status values:

| Port is off - Underload disconnect detected |
| Port is off - Overload detected |
| Port is off - Short detected |
| Port is off - Invalid PD resistor signature detected |
| Port is on - Valid PD resistor signature detected |
| Port is off - Power was denied |
| Port is on - Valid capacitor signature detected |
| Port is off - Backoff state has occurred |
| Port is off - Class error has occurred |

### 25.9 show power inline consumption

Use the `show power inline consumption` EXEC mode command to display information about the inline power consumption for all interfaces or for a specific interface.

**Syntax**

```
show power inline consumption [interface-id| detailed ]
```

**Parameters**

- **Interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.
- **detailed**—Displays information for non-present ports in addition to present ports.
Default Configuration

Show information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following example displays information about the inline power consumption.

```
switchxxxxxx# show power inline consumption

<table>
<thead>
<tr>
<th>Port</th>
<th>Power Limit (W)</th>
<th>Power (W)</th>
<th>Voltage (V)</th>
<th>Current (mA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>15.4</td>
<td>4.115</td>
<td>50.8</td>
<td>81</td>
</tr>
<tr>
<td>gi2</td>
<td>15.4</td>
<td>4.157</td>
<td>50.7</td>
<td>82</td>
</tr>
<tr>
<td>gi3</td>
<td>15.4</td>
<td>4.021</td>
<td>50.9</td>
<td>79</td>
</tr>
</tbody>
</table>
```
26 EEE Commands

26.1 eee enable (global)

Use the `eee enable` Global Configuration command to enable the EEE mode globally. Use the `no` format of the command to disable the mode.

**Syntax**

`eee enable`

`no eee enable`

**Default Configuration**

EEE is enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

In order for EEE to work, the device at the other end of the link must also support EEE and have it enabled. In addition, for EEE to work properly, Auto-Negotiation must be enabled; however, if the port speed is negotiated as 1Giga, EEE always works regardless of the auto-negotiation status (meaning enable or disable).

If Auto-Negotiation is not enabled on the port and its speed is less than 1 Giga, the EEE Operational status is disabled.

**Example**

```
switchxxxxxx(config)# eee enable
```

26.2 eee enable (interface)

Use the `eee enable` Interface Configuration command to enable the EEE mode on an Ethernet port. Use the `no` format of the command to disable the mode.
EEE Commands

Syntax

eee enable
no eee enable

Parameters

N/A

Default Configuration

EEE is enabled.

Command Mode

Interface Configuration mode (Ethernet)

User Guidelines

If Auto-Negotiation is not enabled on the port and its speed is 1 Giga, the EEE Operational status is disabled.

Example

witchxxxxxx(config)#interface gi1
witchxxxxxx(config-if)#eee enable

26.3 eee lldp enable

Use the eee lldp enable Interface Configuration command to enable EEE support by LLDP on an Ethernet port. Use the no format of the command to disable the support.

Syntax

eee lldp enable
no eee lldp enable

Parameters

N/A
Default Configuration
Enabled

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Enabling EEE LLDP advertisement enables devices to choose and change system wake-up times in order to get the optimal energy saving mode.

Example

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)#eee lldp enable
```

26.4 show eee
Use the show eee EXEC command to display EEE information.

Syntax

```
show eee [interface-id]
```

Parameters

interface-id—Specify an interface ID. The interface ID must be an Ethernet port.

Examples

Example 1 - The following displays brief information about all ports

```
switchxxxxxx>show eee
EEE globally enabled
```
EEE Administrate status is enabled on ports: gi1-6, gi7
EEE Operational status is enabled on ports: gi1, gi1-6, gi2, gi5
EEE LLDP Administrate status is enabled on ports: gi1-5
EEE LLDP Operational status is enabled on ports: gi1-5

Example 2 - The following is the information displayed when a port is in state not Present; no information is displayed if the port supports EEE.

switchxxxxxx>show eee gi10
Port Status: notPresent
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Administrate status: enabled

Example 3 - The following is the information displayed when the port is in status DOWN.

switchxxxxxx>show eee gi10
Port Status: DOWN
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
    EEE Administrate status: enabled
    EEE LLDP Administrate status: enabled

Example 4 - The following is the information displayed when the port is in status UP and does not support EEE,

switchxxxxxx>show eee gi2
Port Status: UP
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1Gbps
**Example 5** - The following is the information displayed when the neighbor does not support EEE.

```
switchxxxxxx>show eee gi5
Port Status: UP
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1Gbps
EEE Remote status: disabled
EEE Administrate status: enabled
EEE Operational status: disabled (neighbor does not support)
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

**Example 6** - The following is the information displayed when EEE is disabled on the port.

```
Switch>show eee gi1
Port Status: UP
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1Gbps
EEE Administrate status: disabled
EEE Operational status: disabled
EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled
```

**Example 7** - The following is the information displayed when EEE is running on the port, and EEE LLDP is disabled.

```
switchxxxxxx>show eee gi2
```
Port Status: UP

EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported

Current port speed: 1Gbps

EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled

EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled

Resolved Tx Timer: 10 usec
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec

Example 8 - The following is the information displayed when EEE and EEE LLDP are running on the port.

switchxxxxxx>show eee gi3

Port Status: UP

EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported

Current port speed: 1Gbps

EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled

EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled

Resolved Tx Timer: 10 usec
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Rx Timer: 5 usec
Example 9 - The following is the information displayed when EEE is running on the port, EEE LLDP is enabled but not synchronized with remote link partner.

```
switchxxxxxx>show eee gi9
Port Status: up
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1Gbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 64
Local Tx Timer: 64
Resolved Rx Timer: 16
Local Rx Timer: 16
```

Example 10 - The following is the information displayed when EEE and EEE LLDP are running on the port.

```
switchxxxxxx>show eee gi3
Port Status: UP
EEE capabilities:
    Speed 10M: EEE not supported
    Speed 100M: EEE supported
    Speed 1G: EEE supported
Current port speed: 1Gbps
EEE Remote status: enabled
```
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
Green Ethernet

27.1 green-ethernet energy-detect (global)

Use the `green-ethernet energy-detect` Global Configuration mode command to enable Green-Ethernet Energy-Detect mode globally. Use the `no` form of this command to disable it.

Syntax

```
green-ethernet energy-detect
no green-ethernet energy-detect
```

Parameters

N/A

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# green-ethernet energy-detect
```

27.2 green-ethernet energy-detect (interface)

Use the `green-ethernet energy-detect` Interface configuration mode command to enable green-ethernet Energy-Detect mode on a port. Use the `no` form of this command, to disable it on a port.

Syntax

```
green-ethernet energy-detect
no green-ethernet energy-detect
```
Parameters
N/A

Default Configuration
Enabled

Command Mode
Interface configuration mode (Ethernet)

User Guidelines
Energy-Detect can work only when the port is a copper port. When a port is enabled for auto selection, copper/fiber Energy-Detect cannot work.

It takes the PHY ~5 seconds to fall into sleep mode when the link is lost after normal operation.

Example

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# green-ethernet energy-detect
```

27.3 green-ethernet short-reach (global)

Use the `green-ethernet short-reach` Global Configuration mode command to enable green-ethernet short-reach mode globally. Use the `no` form of this command to disabled it.

Syntax

```
green-ethernet short-reach
no green-ethernet short-reach
```

Parameters
N/A

Default Configuration
Disabled.
Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# green-ethernet short-reach
```

27.4 `green-ethernet short-reach` (interface)

Use the `green-ethernet short-reach` Interface Configuration mode command to enable green-ethernet short-reach mode on a port. Use the `no` form of this command to disable it on a port.

Syntax

```
green-ethernet short-reach
no green-ethernet short-reach
```

Parameters

N/A

Default Configuration

Disabled.

Command Mode

Interface Configuration mode (Ethernet)

User Guidelines

When **Short-Reach** mode is enabled and is not forced, the VCT (Virtual Cable Tester) length check must be performed. The VCT length check can be performed only on a copper port operating at a speed of 1000 Mbps. If the media is not copper or the link speed is not 1000 Mbps, Short-Reach mode is not applied.

When the interface is set to enhanced mode, after the VCT length check has completed and set the power to low, an active monitoring for errors is done continuously. In the case of errors crossing a certain threshold, the PHY will be reverted to long reach.

Note that EEE cannot be enabled if the Short-Reach mode is enabled.
Example

switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# green-ethernet short-reach

27.5  green-ethernet power-meter reset

Use the green-ethernet power-meter reset Privileged EXEC mode command to reset the power save meter.

Syntax

green-ethernet power-meter reset

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode.

Example

switchxxxxxx(config)# green-ethernet power-meter reset

27.6  show green-ethernet

Use the show green-ethernet Privileged EXEC mode command to display green-ethernet configuration and information.

Syntax

show green-ethernet [interface-id | detailed]

Parameters

- interface-id—Specifies an Ethernet port
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**
Display for all ports. If detailed is not used, only present ports are displayed.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
The power savings displayed only includes the power saved by short reach, energy detect and the power saved by disabling the ports LEDs; the EEE power saving is dynamic by nature since it is based on port utilization and is therefore not taken into consideration.

The following describes the reasons for non-operation displayed by this command.

If there are a several reasons, then only the highest priority reason is displayed.

<table>
<thead>
<tr>
<th>Energy-detect Non-operational Reasons</th>
<th>Priority</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>NP</td>
<td>Port is not present</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>LT</td>
<td>Link Type is not supported (fiber, auto media select)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>LU</td>
<td>Port Link is up – NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Short-Reach Non-operational Reasons</th>
<th>Priority</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>NP</td>
<td>Port is not present</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>LT</td>
<td>Link Type is not supported (fiber)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>LS</td>
<td>Link Speed Is not Supported (100M, 10M, 10G)</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>LL</td>
<td>Link Length received from VCT Test exceed threshold</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>LD</td>
<td>Port Link is Down – NA</td>
</tr>
</tbody>
</table>
Example

(If a mode is not supported, its columns are removed from the output).

switchxxxxxx# show green-ethernet

Energy-Detect mode: Enabled
Short-Reach mode: Disabled
Disable Port LEDs mode: Enabled
Power Consumption: 76% (3.31W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
Short-Reach cable length threshold: 50m

<table>
<thead>
<tr>
<th>Port</th>
<th>Energy-Detect</th>
<th>Short-Reach</th>
<th>VCT Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Admin Oper Reason</td>
<td>Admin Force Oper Reason</td>
<td>Length</td>
</tr>
<tr>
<td>151</td>
<td>on</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>152</td>
<td>off LU</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>153</td>
<td>off LU</td>
<td>off</td>
<td>off</td>
</tr>
</tbody>
</table>
28.1 channel-group

Use the channel-group Interface Configuration (Ethernet) mode command to associate a port with a port-channel. Use the no form of this command to remove a port from a port-channel.

Syntax

channel-group port-channel mode {on | auto}

no channel-group

Parameters

- port-channel—Specifies the port channel number for the current port to join.
- mode—Specifies the mode of joining the port channel. The possible values are:
  - on—Forces the port to join a channel without an LACP operation.
  - auto—Forces the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

Default mode is on.

Example

The following example forces port gi1 to join port-channel 1 without an LACP operation.

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# channel-group 1 mode on
```
28.2 port-channel load-balance

Use the `port-channel load-balance` Global Configuration mode command to configure the load balancing policy of the port channeling. Use the `no` form of this command to reset to default.

**Syntax**

```
port-channel load-balance {src-dst-mac| src-dst-mac-ip}
no port-channel load-balance
```

**Parameters**

- `src-dst-mac`—Port channel load balancing is based on the source and destination MAC address.
- `src-dst-mac-ip`—Port channel load balancing is based on the source and destination of MAC and IP addresses.

**Default Configuration**

src-dst-mac is the default option.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# port-channel load-balance src-dst-mac
switchxxxxxx(config)# port-channel load-balance src-dst-mac-ip
```

28.3 show interfaces port-channel

Use the `show interfaces port-channel` EXEC mode command to display port-channel information for all port channels or for a specific port channel.

**Syntax**

```
show interfaces port-channel [interface-id]
```
Parameters

interface-id—Specify an interface ID. The interface ID must be a Port Channel.

Command Mode

EXEC mode

Examples

Example 1 - The following example displays information on all port-channels.

```
switchxxxxxx# show interfaces port-channel
Load balancing: src-dst-mac.
Gathering information...
Channel Ports
-------  -----  
Po1      Active: gi1,Inactive: gi2-3
Po2      Active: gi5 Inactive: gi4
```

Example 2 - The following example displays information on port-channels containing port 1

```
switchxxxxxx# show interfaces switchport gi1
Gathering information...
Name: gi1
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: 1
2-4094 (Inactive)
General PVID: 1
General VLANs Enabled: none
```
General Egress Tagged VLANs Enabled: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs Enabled: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN Enabled: none
DVA: disable
29.1 bridge multicast filtering

Use the `bridge multicast filtering` Global Configuration mode command to enable the filtering of Multicast addresses. Use the `no` form of this command to disable Multicast address filtering.

**Syntax**

```
bridge multicast filtering
no bridge multicast filtering
```

**Default Configuration**

Multicast address filtering is disabled. All Multicast addresses are flooded to all ports.

**Command Mode**

Global Configuration mode

**User Guidelines**

When this feature is enabled, unregistered Multicast traffic (as opposed to registered) will still be flooded.

All registered Multicast addresses will be forwarded to the Multicast groups. There are two ways to manage Multicast groups, one is the IGMP Snooping feature, and the other is the `bridge multicast forward-all` command.

**Example**

The following example enables bridge Multicast filtering.

```
switchxxxxxx(config)# bridge multicast filtering
```
29.2 bridge multicast mode

Use the **bridge multicast mode** Interface Configuration (VLAN) mode command to configure the Multicast bridging mode. Use the **no** form of this command to return to the default configuration.

**Syntax**

`bridge multicast mode {mac-group / ip-group / ip-src-group}`

`no bridge multicast mode`

**Parameters**

- **mac-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address.
- **ipv4-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN and IPv4 destination address for IPv4 packets.
- **ipv4-src-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN, IPv4 destination address and IPv4 source address for IPv4 packets.

**Default Configuration**

The default mode is mac-group.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Use the mac-group option when using a network management system that uses a MIB based on the Multicast MAC address. Otherwise, it is recommended to use the ipv4-group or ipv4-src-group mode, because there is no overlapping of IPv4 Multicast addresses in these modes.
For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries in the FDB, as described in the following table:

<table>
<thead>
<tr>
<th>FDB Mode</th>
<th>CLI Commands</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>bridge multicast address</td>
<td>bridge multicast forbidden address</td>
</tr>
<tr>
<td>ipv4-group</td>
<td>bridge multicast ip-address</td>
<td>bridge multicast forbidden ip-address</td>
</tr>
<tr>
<td>ipv4-src-group</td>
<td>bridge multicast source group</td>
<td>bridge multicast forbidden source group</td>
</tr>
</tbody>
</table>

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the IGMP version that is used in the network:

<table>
<thead>
<tr>
<th>FDB mode</th>
<th>IGMP version 2</th>
<th>IGMP version 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>MAC group address</td>
<td>MAC group address</td>
</tr>
<tr>
<td>ipv4-group</td>
<td>IP group address</td>
<td>IP group address</td>
</tr>
<tr>
<td>ipv4-src-group</td>
<td>(*)</td>
<td>IP source and group addresses</td>
</tr>
</tbody>
</table>

(*) Note that (*,G) cannot be written to the FDB if the mode is ipv4-src-group. In that case, no new FDB entry is created, but the port is added to the static (S,G) entries (if they exist) that belong to the requested group. It is recommended to set the FDB mode to ipv4-group or mac-group for IGMP version 2.

If an application on the device requests (*,G), the operating FDB mode is changed to ipv4-group.

**Example**

The following example configures the Multicast bridging mode as an ipv4-group on VLAN 2.

```bash
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast mode ipv4-group
```
29.3  bridge multicast address

Use the **bridge multicast address** Interface Configuration (VLAN) mode command to register a MAC-layer Multicast address in the bridge table and statically add or remove ports to or from the group. Use the **no** form of this command to unregister the MAC address.

**Syntax**

```
bridge multicast address {mac-multicast-address | ipv4-multicast-address} [[add | remove] {ethernet interface-list | port-channel port-channel-list}]
no bridge multicast address {mac-multicast-address}
```

**Parameters**

- **mac-multicast-address | ipv4-multicast-address**—Specifies the group Multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

No Multicast addresses are defined.

If **ethernet interface-list** or **port-channel port-channel-list** is specified without specifying **add** or **remove**, the default option is **add**.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

To register the group in the bridge database without adding or removing ports or port channels, specify the **mac-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.
You can execute the command before the VLAN is created.

**Examples**

**Example 1** - The following example registers the MAC address to the bridge table:

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

**Example 2** - The following example registers the MAC address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03 add gi1-2
```

### 29.4 bridge multicast forbidden address

Use the `bridge multicast forbidden address` Interface Configuration (VLAN) mode command to forbid adding or removing a specific Multicast address to or from specific ports. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
bridge multicast forbidden address {mac-multicast-address | ipv4-multicast-address} [add | remove] {ethernet interface-list | port-channel port-channel-list}
```

```
o bridge multicast forbidden address {mac-multicast-address}
```

**Parameters**

- `mac-multicast-address | ipv4-multicast-address`—Specifies the group Multicast address.
- `add`—Forbids adding ports to the group.
- `remove`—Forbids removing ports from the group.
- `ethernet interface-list`—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
• **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**Default Configuration**

No forbidden addresses are defined.
Default option is **add**.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Before defining forbidden ports, the Multicast group should be registered, using **bridge multicast address**.

You can execute the command before the VLAN is created.

**Example**

The following example forbids MAC address 0100.5e02.0203 on port **gi9** within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 0100.5e02.0203
switchxxxxxx(config-if)# bridge multicast forbidden address 0100.5e02.0203 add gi9
```

**29.5 bridge multicast ip-address**

Use the **bridge multicast ip-address** Interface Configuration (VLAN) mode command to register IP-layer Multicast addresses to the bridge table, and statically add or remove ports to or from the group. Use the no form of this command to unregister the IP address.

**Syntax**

```
bridge multicast ip-address ip-multicast-address [[add | remove] [ethernet interface-list] | port-channel port-channel-list]
```

```
no bridge multicast ip-address ip-multicast-address
```
Parameters

- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

Default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **ip-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Example

The following example registers the specified IP address to the bridge table:

```bash
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
```

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

```bash
switchxxxxxx(config)# interface vlan 8
```
29.6 bridge multicast forbidden ip-address

Use the bridge multicast forbidden ip-address Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP Multicast address to or from specific ports. Use the no form of this command to restore the default configuration.

Syntax

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

no bridge multicast forbidden ip-address {ip-multicast-address}

Parameters

- ip-multicast-address—Specifies the group IP Multicast address.
- add—Forbids adding ports to the group.
- remove—Forbids removing ports from the group.
- ethernet interface-list—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.
Example

The following example registers IP address 239.2.2.2, and forbids the IP address on port gi9 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden ip-address 239.2.2.2 add gi9
```

29.7 **bridge multicast source group**

Use the **bridge multicast source group** Interface Configuration (VLAN) mode command to register a source IP address - Multicast IP address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the no form of this command to unregister the source-group-pair.

**Syntax**

```
bridge multicast source ip-address group ip-multicast-address [add | remove] [ethernet interface-list | port-channel port-channel-list]
no bridge multicast source ip-address group ip-multicast-address
```

**Parameters**

- **ip-address**—Specifies the source IP address.
- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Adds ports to the group for the specific source IP address.
- **remove**—Removes ports from the group for the specific source IP address.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

No Multicast addresses are defined.
The default option is **add**.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

The following example registers a source IP address - Multicast IP address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
```

### 29.8 bridge multicast forbidden source group

Use the `bridge multicast forbidden source group` Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP source address - Multicast address pair to or from specific ports. Use the no form of this command to return to the default configuration.

**Syntax**

```
bridge multicast forbidden source ip-address group ip-multicast-address {add | remove} {ethernet interface-list | port-channel port-channel-list}
no bridge multicast forbidden source ip-address group ip-multicast-address
```

**Parameters**

- **ip-address**—Specifies the source IP address.
- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Forbids adding ports to the group for the specific source IP address.
- **remove**—Forbids removing ports from the group for the specific source IP address.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

No forbidden addresses are defined.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

**Example**

The following example registers a source IP address - Multicast IP address pair to the bridge table, and forbids adding the pair to port gi9 on VLAN 8:

```plaintext
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden source 13.16.1.1 group 239.2.2.2 add gi9
```

**29.9 bridge multicast ipv6 mode**

Use the **bridge multicast ipv6 mode** Interface Configuration (VLAN) mode command to configure the Multicast bridging mode for IPv6 Multicast packets. Use the no form of this command to return to the default configuration.

**Syntax**

bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}

no bridge multicast ipv6 mode
Parameters

- **mac-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC destination address.
- **ip-group**—Specifies that Multicast bridging is based on the packet's VLAN and IPv6 destination address for IPv6 packets.
- **ip-src-group**—Specifies that Multicast bridging is based on the packet's VLAN, IPv6 destination address and IPv6 source address for IPv6 packets.

Default Configuration

The default mode is **mac-group**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the **mac-group** mode when using a network management system that uses a MIB based on the Multicast MAC address.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries for IPv6 Multicast addresses in the FDB, as described in the following table:

<table>
<thead>
<tr>
<th>FDB Mode</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>bridge multicast address</td>
</tr>
<tr>
<td></td>
<td>bridge multicast forbidden address</td>
</tr>
<tr>
<td>ipv6-group</td>
<td>bridge multicast ipv6 ip-address</td>
</tr>
<tr>
<td></td>
<td>bridge multicast ipv6 forbidden ip-address</td>
</tr>
<tr>
<td>ipv6-src-group</td>
<td>bridge multicast ipv6 source group</td>
</tr>
<tr>
<td></td>
<td>bridge multicast ipv6 forbidden source group</td>
</tr>
</tbody>
</table>

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the MLD version that is used in the network:(*)

<table>
<thead>
<tr>
<th>FDB mode</th>
<th>MLD version 1</th>
<th>MLD version 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-group</td>
<td>MAC group address</td>
<td>MAC group address</td>
</tr>
<tr>
<td>ipv6-group</td>
<td>IPv6 group address</td>
<td>IPv6 group address</td>
</tr>
<tr>
<td>ipv6-src-group</td>
<td>('*) IPv6 source and group addresses</td>
<td>IPv6 source and group addresses</td>
</tr>
</tbody>
</table>
Note that (*,G) cannot be written to the FDB if the mode is `ip-src-group`. In that case, no new FDB entry is created, but the port is added to the (S,G) entries (if they exist) that belong to the requested group. If an application on the device requests (*,G), the operating FDB mode is changed to `ip-group`.

You can execute the command before the VLAN is created.

**Example**

The following example configures the Multicast bridging mode as an `ip-group` on VLAN 2.

```shell
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast ipv6 mode ip-group
```

### 29.10 bridge multicast ipv6 ip-address

Use the `bridge multicast ipv6 ip-address` Interface Configuration (VLAN) mode command to register an IPv6 Multicast address to the bridge table, and statically add or remove ports to or from the group. Use the `no` form of this command to unregister the IPv6 address.

**Syntax**

```
bridge multicast ipv6 ip-address ipv6-multicast-address [add | remove] [ethernet interface-list / port-channel port-channel-list]
no bridge multicast ipv6 ip-address ip-multicast-address
```

**Parameters**

- **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.
Default Configuration

No Multicast addresses are defined.
The default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **ipv6-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Examples

**Example 1** - The following example registers the IPv6 address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
```

**Example 2** - The following example registers the IPv6 address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
   add gi1-2
```

**29.11 bridge multicast ipv6 forbidden ip-address**

Use the **bridge multicast ipv6 forbidden ip-address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 Multicast address to or from specific ports. To restore the default configuration, use the **no** form of this command.
Syntax

bridge multicast ipv6 forbidden ip-address {ipv6-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}

no bridge multicast ipv6 forbidden ip-address {ipv6-multicast-address}

Parameters

- **ipv6-multicast-address**—Specifies the group IPv6 Multicast address.
- **add**—Forbids adding ports to the group.
- **remove**—Forbids removing ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

The default option is add.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers an IPv6 Multicast address, and forbids the IPv6 address on port gi9 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
```
29.12 bridge multicast ipv6 source group

Use the `bridge multicast ipv6 source group` Interface Configuration (VLAN) mode command to register a source IPv6 address - Multicast IPv6 address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the no form of this command to unregister the source-group-pair.

**Syntax**

```
bridge multicast ipv6 source ipv6-source-address group ipv6-multicast-address
[ [add | remove] [ethernet interface-list | port-channel port-channel-list] ]
```

**Parameters**

- `ipv6-source-address`—Specifies the source IPv6 address.
- `ipv6-multicast-address`—Specifies the group IPv6 Multicast address.
- `add`—Adds ports to the group for the specific source IPv6 address.
- `remove`—Removes ports from the group for the specific source IPv6 address.
- `ethernet interface-list`—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- `port-channel port-channel-list`—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**Default Configuration**

No Multicast addresses are defined.

The default option is add.

**Command Mode**

Interface Configuration (VLAN) mode
Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group FF00:0:0:0:4:4:4:1
```

29.13 bridge multicast ipv6 forbidden source group

Use the `bridge multicast ipv6 forbidden source group` Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 source address - Multicast address pair to or from specific ports. Use the `no` form of this command to return to the default configuration.

Syntax

```
bridge multicast ipv6 forbidden source ipv6-source-address group ipv6-multicast-address {add | remove} {ethernet interface-list | port-channel port-channel-list}
```

```
no bridge multicast ipv6 forbidden source ipv6-address group ipv6-multicast-address
```

Parameters

- `ipv6-source-address`—Specifies the source IPv6 address.
- `ipv6-multicast-address`—Specifies the group IPv6 multicast address.
- `add`—Forbids adding ports to the group for the specific source IPv6 address.
- `remove`—Forbids removing ports from the group for the specific source IPv6 address.
- `ethernet interface-list`—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- `port-channel port-channel-list`—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.
Default Configuration
No forbidden addresses are defined.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Before defining forbidden ports, the Multicast group should be registered.
You can execute the command before the VLAN is created.

Example
The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table, and forbids adding the pair to gi9 on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4:1 group FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)# bridge multicast forbidden source 2001:0:0:0:4:4:4:1 group FF00:0:0:0:4:4:4:1 add gi9
```

29.14 bridge multicast unregistered
Use the bridge multicast unregistered Interface Configuration (Ethernet, Port-Channel) mode command to configure forwarding unregistered Multicast addresses. Use the no form of this command to restore the default configuration.

Syntax
bridge multicast unregistered [forwarding / filtering]
no bridge multicast unregistered

Parameters
- **forwarding**—Forwards unregistered Multicast packets.
- **filtering**—Filters unregistered Multicast packets.
Default Configuration
Unregistered Multicast addresses are forwarded.

Command Mode
Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines
Do not enable unregistered Multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

Example
The following example specifies that unregistered Multicast packets are filtered on gi1:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# bridge multicast unregistered filtering
```

29.15 bridge multicast forward-all

Use the bridge multicast forward-all Interface Configuration (VLAN) mode command to enable forwarding all multicast packets for a range of ports or port channels. Use the no form of this command to restore the default configuration.

Syntax

```
bridge multicast forward-all
  [add | remove] (ethernet interface-list | port-channel port-channel-list)
```

Parameters
- **add**—Forces forwarding of all Multicast packets.
- **remove**—Does not force forwarding of all Multicast packets.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**Default Configuration**

Forwarding of all Multicast packets is disabled.

**Command Mode**

Interface Configuration (VLAN) mode

**Example**

The following example enables all Multicast packets on port gi8 to be forwarded.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forward-all add gi8
```

**29.16 bridge multicast forbidden forward-all**

Use the `bridge multicast forbidden forward-all` Interface Configuration (VLAN) mode command to forbid a port to dynamically join Multicast groups. Use the no form of this command to restore the default configuration.

**Syntax**

```
bridge multicast forbidden forward-all [add | remove] [ethernet interface-list | port-channel port-channel-list]
```

**Parameters**

- **add**—Forbids forwarding of all Multicast packets.
- **remove**—Does not forbid forwarding of all Multicast packets.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- `port-channel port-channel-list`—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**Default Configuration**

Ports are not forbidden to dynamically join Multicast groups.

The default option is `add`.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

Use this command to forbid a port to dynamically join (by IGMP, for example) a Multicast group.

The port can still be a Multicast router port.

**Example**

The following example forbids forwarding of all Multicast packets to gi1 within VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forbidden forward-all add ethernet gi1
```

### 29.17 bridge unicast unknown

Use the `bridge unicast unknown` Interface Configuration mode command to enable egress filtering of Unicast packets where the destination MAC address is unknown to the device. Use the no form of this command to restore the default configuration.

**Syntax**

```
bridge unicast unknown {filtering | forwarding}
no bridge unicast unknown
```
Parameters

- **filtering**— Filter unregistered Unicast packets.
- **forwarding**— Forward unregistered Unicast packets.

Default Configuration

Forwarding.

Command Mode

Interface Configuration mode

Example

The following example drops Unicast packets on VLAN 2 when the destination is unknown.

```
switchxxxxxxx(config)# interface vlan 2
switchxxxxxxx(config-if)# bridge unicast unknown filtering
```

### 29.18  mac address-table static

Use the **mac address-table static** Global Configuration mode command to add a MAC-layer station source address to the MAC address table. Use the **no** form of this command to delete the MAC address.

**Syntax**

```
mac address-table static mac-address vlan vlan-id interface interface-id [permanent /delete-on-reset /delete-on-timeout /secure]
```

```
no mac address-table static [mac-address] vlan vlan-id
```

**Parameters**

- **mac-address**— MAC address (Range: Valid MAC address)
- **vlan-id**— Specify the VLAN
- **interface-id**— Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: valid ethernet port, valid port-channel)
Address Table Commands

- **permanent**— The permanent static MAC address. The keyword is applied by the default.
- **delete-on-reset**— The delete-on-reset static MAC address.
- **delete-on-timeout**— The delete-on-timeout static MAC address.
- **secure**— The secure MAC address. May be used only in a secure mode.

**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 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 value of time-of-live is supported:

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

The following types are supported:

- **static**— MAC address manually added by the command with the following keywords specifying its time-of-live:
  - **permanent**
  - **delete-on-reset**
  - **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 non secure mode. A value of its time-to-live attribute is `delete-on-timeout`.

### Examples

**Example 1** - The following example adds two permanent static MAC address:

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

**Example 2** - The following example adds a deleted-on-reset static MAC address:

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

**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 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 gi1 secure
```

### 29.19 clear mac address-table

Use the `clear mac address-table` Privileged EXEC command to remove learned or secure entries from the forwarding database (FDB).
Syntax

clear mac address-table dynamic [interface interface-id]
clear mac address-table secure interface interface-id

Parameters

- **dynamic interface interface-id**—Delete all dynamic (learned) addresses on the specified interface. The interface ID can be one of the following types: Ethernet port or port-channel. If interface ID is not supplied, all dynamic addresses are deleted.

- **secure interface interface-id**—Delete all the secure addresses learned on the specific interface. A secure address on a MAC address learned on ports on which port security is defined.

Default Configuration

For dynamic addresses, if interface-id is not supplied, all dynamic entries are deleted.

Command Mode

Privileged EXEC mode

Examples

Example 1 - Delete all dynamic entries from the FDB.

```plaintext
switchxxxxxx# clear mac address-table dynamic
```

Example 2 - Delete all secure entries from the FDB learned on secure port gi1.

```plaintext
switchxxxxxx# clear mac address-table secure interface gi1
```

29.20  show bridge unicast unknown

Use the **show bridge unicast unknown** command to display the unknown Unicast filtering configuration.
### Syntax

```
show bridge unicast unknown [interface-id]
```

### Parameters

**interface-id**—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel

### Default

### Command Mode

EXEC

### Example

```
switchxxxxxx# show bridge unicast unknown

Port    Unregistered
------   -------------
1/1      Forward
1/2      Filter
1/3      Filter
```

### 29.21  mac address-table aging-time

Use the `mac address-table aging-time` Global configuration command to set the aging time of the address table. Use the `no` form of this command to restore the default.

#### Syntax

```
mac address-table aging-time seconds
no mac address-table aging-time
```

#### Parameters

**seconds**—Time is number of seconds. (Range: 10–10-630)
Default Configuration

300

Command Mode

Global Configuration mode

Example

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

29.22  port security

Use the port security Interface Configuration (Ethernet, Port-channel) mode command to enable port security learning mode on an interface. Use the no form of this command to disable port security learning mode on an interface.

Syntax

port security [forward /discard /discard-shutdown] [trap seconds]

no port security

Parameters

- **forward**—Forwards packets with unlearned source addresses, but does not learn the address.
- **discard**—Discards packets with unlearned source addresses.
- **discard-shutdown**—Discards packets with unlearned source addresses and shuts down the port.
- **trap seconds**—Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

Default Configuration

The feature is disabled by default.

The default mode is **discard**.

The default number of seconds is zero, but if **traps** is entered, a number of seconds must also be entered.
Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

See the bridge unicast unknown command for information about MAC address attributes (type and time-to-live) definitions.

When the 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 port security command enables a mode on a port differing from the lock mode all dynamic addresses learned on the port are deleted.

When the no port security command cancels a secure mode on a port all secure addresses defined on the port are changed to dynamic addresses.

Additionally to set a mode, use the port security command to set an action that the switch should perform on a frame which source MAC address cannot be learned.

Example

The following example forwards all packets to port gi1 without learning addresses of packets from unknown sources and sends traps every 100 seconds, if a packet with an unknown source address is received.

```
switchxxxxxx(config) interface gi7
switchxxxxxx(config-if) port security mode lock
switchxxxxxx(config-if) port security forward trap 100
switchxxxxxx(config-if) exit
```

29.23 port security mode

Use the port security mode Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. Use the no form of this command to restore the default configuration.

Syntax

- `port security mode [max-addresses | lock | secure permanent |secure delete-on-reset]`
no port security mode

Parameters

- **max-addresses**— Non secure mode with limited learning dynamic MAC addresses. The static MAC addresses may be added on the port manually by the `bridge unicast unknown` command.

- **lock**— Secure mode without MAC learning. The static and secure MAC addresses may be added on the port manually by the `bridge unicast unknown` command.

- **secure permanent**— Secure mode with limited learning permanent secure MAC addresses with the `permanent` time-of-live. The static and secure MAC addresses may be added on the port manually by the `mac address-table static` command.

- **secure delete-on-reset**— Secure mode with limited learning secure MAC addresses with the `delete-on-reset` time-of-live. The static and secure MAC addresses may be added on the port manually by the `mac address-table static` command.

Default Configuration

The default port security mode is **lock**.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The default port mode is called regular. In this mode, the port allows unlimited learning of dynamic addresses. The static MAC addresses may be added on the port manually by the `bridge unicast unknown` command.

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use the `port security mode` command to change the default mode before the `port security mode` command.

Example

The following example sets the port security mode to Lock for gi7.

```
switchxxxxxx(config)interface gi7
```
29.24  port security max

Use the port security max Interface Configuration (Ethernet, Port-channel) mode command to configure the maximum number of addresses that can be learned on the port while the port is in port, max-addresses or secure mode. Use the no form of this command to restore the default configuration.

Syntax

port security max max-addr

no port security max

Parameters

max-addr—Specifies the maximum number of addresses that can be learned on the port. (Range: 0–256)

Default Configuration

This default maximum number of addresses is 1.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use this command to change the default value before the port security command.

Example

The following example sets the port to limited learning mode:

switchxxxxxx(config)#interface gi7
switchxxxxxx(config-if)port security mode max
Address Table Commands

switchxxxxxxx(config-if)port security max 20
switchxxxxxxx(config-if)port security
switchxxxxxxx(config-if)exit

29.25  show mac address-table

Use the show mac address-table EXEC command to view entries in the MAC address table.

Syntax

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

Parameters

- **dynamic**—Displays only dynamic MAC address table entries.
- **static**—Displays only static MAC address table entries.
- **secure**—Displays only secure MAC address table entries.
- **vlan**—Displays entries for a specific VLAN.
- **interface-id**—Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **mac-address**—Displays entries for a specific MAC address.

Default Configuration

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

Command Mode

EXEC mode

User Guidelines

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

Example 1 - Displays entire address table.

```
switchxxxxxx# show mac address-table
Aging time is 300 sec

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:00:26:08:13:23</td>
<td>0</td>
<td>self</td>
</tr>
<tr>
<td>1</td>
<td>00:3f:bd:45:5a:b1</td>
<td>gi1</td>
<td>static</td>
</tr>
<tr>
<td>1</td>
<td>00:a1:b0:69:63:f3</td>
<td>gi4</td>
<td>dynamic</td>
</tr>
<tr>
<td>2</td>
<td>00:a1:b0:69:63:f3</td>
<td>gi5</td>
<td>dynamic</td>
</tr>
</tbody>
</table>
```

Example 2 - Displays address table entries containing the specified MAC address.

```
switchxxxxxx# show mac address-table 00:3f:bd:45:5a:b1
Aging time is 300 sec

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:3f:bd:45:5a:b1</td>
<td>static</td>
<td>gi9</td>
</tr>
</tbody>
</table>
```

29.26 show mac address-table count

Use the `show mac address-table count` EXEC mode command to display the number of addresses present in the Forwarding Database.

Syntax

```
show mac address-table count [vlan vlan / interface interface-id]
```

Parameters

- **vlan**—Specifies VLAN.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
Command Mode
EXEC mode

Example

switchxxxxxx# show mac address-table count
Capacity: 8192
Free: 8083
Used: 109
Secure : 0
Dynamic : 25
Static : 1
Internal : 0

29.27 show bridge multicast mode
Use the show bridge multicast mode EXEC mode command to display the Multicast bridging mode for all VLANs or for a specific VLAN.

Syntax
show bridge multicast mode [vlan vlan-id]

Parameters
vlan vlan-id—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays the Multicast bridging mode for all VLANs.

switchxxxxxx# show bridge multicast mode
### 29.28 show bridge multicast address-table

Use the `show bridge multicast address-table` EXEC mode command to display Multicast MAC addresses or IP Multicast address table information.

**Syntax**

```
show bridge multicast address-table [vlan vlan-id] [address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}] [format {ip | mac}] [source {ipv4-source-address | ipv6-source-address}]
```

**Parameters**

- **vlan-id vlan-id**—Display entries for specified VLAN ID.
- **address**—Display entries for specified Multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC Multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 Multicast address.
  - **ipv6-multicast-address**— Specifies the IPv6 Multicast address.
- **format**—(this applies if picked mac-multicast-address), then i can display it either in mac or ip format) Display entries for specified Multicast address format. The possible values are:
  - **ip**—Specifies that the Multicast address is an IP address.
  - **mac**— Specifies that the Multicast address is a MAC address.
- **source {ipv4-source-address | ipv6-source-address}**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**— Specifies the source IPv6 address.
Default Configuration

If the format is not specified, it defaults to mac (only if mac-multicast-address was entered).

If VLAN ID is not entered, entries for all VLANs are displayed.

If MAC or IP address is not supplied, entries for all addresses are displayed.

Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast router ports (defined statically or discovered dynamically) are members in all MAC groups.

Ports that were defined via the bridge multicast forbidden forward-all command are displayed in all forbidden MAC entries.

Changing the Multicast mode can move static Multicast addresses that are written in the device FDB to a shadow configuration because of FDB hash collisions.

Example

The following example displays bridge Multicast address information.

switchxxxxxx# show bridge multicast address-table

Multicast address table for VLANs in MAC-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>01:00:5e:02:02:03</td>
<td>Static</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>01:00:5e:02:02:03</td>
<td>gi9</td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv4-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>232.5.6.5</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>233.22.2.6</td>
<td></td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224.2.2.251</td>
<td>11.2.2.3</td>
<td>Dynamic</td>
<td>gi1</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>239.2.2.2</td>
<td>*</td>
<td>gi9</td>
</tr>
<tr>
<td>8</td>
<td>239.2.2.2</td>
<td>1.1.1.11</td>
<td>gi9</td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv6-GROUP bridging mode:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP/MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>Static</td>
<td>gi1-2, gi7, Po1</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP/MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>gi9</td>
</tr>
</tbody>
</table>

Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>*</td>
<td>Static</td>
<td>gi1-2, gi7, Po1</td>
</tr>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>fe80::200:7ff</td>
<td>Static</td>
<td>fe00:200</td>
</tr>
</tbody>
</table>

Forbidden ports for Multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>*</td>
<td>gi1-2, gi7, Po1</td>
</tr>
<tr>
<td>8</td>
<td>ff02::4:4:4</td>
<td>fe80::200:7ff</td>
<td>gi1-2, gi7, Po1</td>
</tr>
</tbody>
</table>
---- --------------- --------------- ----------
8   ff02::4:4:4     *               gi9
8   ff02::4:4:4     fe80::200:7ff:f    gi9
e00:200

29.29  show bridge multicast address-table static

Use the **show bridge multicast address-table static** EXEC mode command to display the statically configured Multicast addresses.

**Syntax**

```
show bridge multicast address-table static [vlan vlan-id] [address mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address] [source ipv4-source-address | ipv6-source-address] [all | mac | ip]
```

**Parameters**

- **vlan vlan-id**—Specifies the VLAN ID.
- **address**—Specifies the Multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC Multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 Multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 Multicast address.
- **source**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

**Default Configuration**

When **all/mac/ip** is not specified, all entries (MAC and IP) will be displayed.

**Command Mode**

EXEC mode

**User Guidelines**

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000—0100.5e7f.ffff.
### Example
The following example displays the statically configured Multicast addresses.

```
switchxxxxxx# show bridge multicast address-table static
```

**MAC-GROUP table**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td>0100.9923.0787</td>
<td>gi1, gi2</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------------</td>
<td>---------</td>
</tr>
</tbody>
</table>

**IPv4-GROUP Table**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td>231.2.2.3</td>
<td>gi1, gi2</td>
</tr>
<tr>
<td>19</td>
<td>231.2.2.8</td>
<td>gi-8</td>
</tr>
<tr>
<td>19</td>
<td>231.2.2.8</td>
<td>gi9-21</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td>231.2.2.3</td>
<td>gi8</td>
</tr>
<tr>
<td>19</td>
<td>231.2.2.8</td>
<td>gi3</td>
</tr>
</tbody>
</table>

**IPv4-SRC-GROUP Table**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>---------------</td>
<td>----------------</td>
<td>-------</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>---------------</td>
<td>----------------</td>
<td>-------</td>
</tr>
</tbody>
</table>

**IPv6-GROUP Table**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>191</td>
<td>FF12::8</td>
<td>gi1-8</td>
</tr>
</tbody>
</table>
### 29.30 show bridge multicast filtering

Use the **show bridge multicast filtering** EXEC mode command to display the Multicast filtering configuration.

**Syntax**

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

**Parameters**

`vlan-id`—Specifies the VLAN ID. (Range: Valid VLAN)

**Default Configuration**

N/A

**Command Mode**

EXEC mode

---

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>FF12::3</td>
<td>gi8</td>
</tr>
<tr>
<td>191</td>
<td>FF12::8</td>
<td>gi8</td>
</tr>
</tbody>
</table>

IPv6-SRC-GROUP Table:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>192</td>
<td>FF12::8</td>
<td>FE80::201:C9A9:FE40:8988</td>
<td>gi1-8</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group Address</th>
<th>Source address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>192</td>
<td>FF12::3</td>
<td>FE80::201:C9A9:FE40:8988</td>
<td>gi8</td>
</tr>
</tbody>
</table>
Example

The following example displays the Multicast configuration for VLAN 1.

```
switchxxxxxx# show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1
Port         Forward-All
------       ------
-----       Static Status
gi1         --------   ------
   gi2      Forbidden Filter
   gi3      Forward    Forward(s)
   -        Forward(d)
```

29.31 show bridge multicast unregistered

Use the **show bridge multicast unregistered** EXEC mode command to display the unregistered Multicast filtering configuration.

Syntax

```
show bridge multicast unregistered [interface-id]
```

Parameters

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display for all interfaces.

Command Mode

EXEC mode
Example
The following example displays the unregistered Multicast configuration.

```
switchxxxxxx# show bridge multicast unregistered
Port Unregistered
------- ---------------
    gi1  Forward
    gi2  Filter
    gi3  Filter
```

29.32 show ports security
Use the `show ports security` Privileged EXEC mode command to display the port-lock status.

Syntax
`show ports security [interface-id | detailed]`

Parameters
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration
Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode
Privileged EXEC mode

Example
The following example displays the port-lock status of all ports.

```
switchxxxxxx# show ports security
```

The following table describes the fields shown above.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Status</td>
<td>The port security status. The possible values are: Enabled or Disabled.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken on violation.</td>
</tr>
<tr>
<td>Maximum</td>
<td>The maximum number of addresses that can be associated on this port in the Max-Addresses mode.</td>
</tr>
<tr>
<td>Trap</td>
<td>The status of SNMP traps. The possible values are: Enable or Disable.</td>
</tr>
<tr>
<td>Frequency</td>
<td>The minimum time interval between consecutive traps.</td>
</tr>
</tbody>
</table>

### 29.33 show ports security addresses

Use the `show ports security addresses` Privileged EXEC mode command to display the current dynamic addresses in locked ports.

**Syntax**

```
show ports security addresses [interface-id | detailed]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.
Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays dynamic addresses in all currently locked port:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Learning</th>
<th>Current</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>gi2</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi3</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi4</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi5</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi6</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi7</td>
<td>Disabled</td>
<td>Lock</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

29.34 bridge multicast reserved-address

Use the `bridge multicast reserved-address` Global Configuration mode command to define the action on Multicast reserved-address packets. Use the `no` form of this command to revert to default.

Syntax

`bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype | llc sap | llc-snap pid] [discard | bridge]`

`no bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype | llc sap | llc-snap pid]`
Parameters

- **mac-multicast-address**—MAC Multicast address in the reserved MAC addresses range. (Range: 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-2F)
- **ethernet-v2 ethtype**—Specifies that the packet type is Ethernet v2 and the Ethernet type field (16 bits in hexadecimal format). (Range: 0x0600–0xFFFF)
- **llc sap**—Specifies that the packet type is LLC and the DSAP-SSAP field (16 bits in hexadecimal format). (Range: 0xFFFF)
- **llc-snap pid**—Specifies that the packet type is LLC-SNAP and the PID field (40 bits in hexadecimal format). (Range: 0x0000000000 - 0xFFFFFFFFFF)
- **discard**—Specifies discarding the packets.
- **bridge**—Specifies bridging (forwarding) the packets

Default Configuration

- If the user-supplied MAC Multicast address, ethtype and encapsulation (LLC) specifies a protocol supported on the device (called Peer), the default action (discard or bridge) is determined by the protocol.
- If not, the default action is as follows:
  - For MAC addresses in the range 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-0F, the default is **discard**.
  - For MAC addresses in the range 00-80-C2-00-00-10–01-80-C2-00-00-2F, the default is **bridge**.

Command Mode

Global Configuration mode

User Guidelines

If the packet/service type (ethertype/encapsulation) is not specified, the configuration is relevant to all the packets with the configured MAC address.

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

The packets that are bridged are subject to security ACLs.

The actions define by this command has precedence over forwarding rules defined by applications/protocols (STP, LLDP etc.) supported on the device.
29.35  show bridge multicast reserved-addresses

Use the show bridge multicast reserved-addresses EXEC mode command to display the Multicast reserved-address rules.

Syntax

show bridge multicast reserved-addresses

Command Mode

EXEC mode

Example

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

switchxxxxxx # show bridge multicast reserved-addresses

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Frame Type</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-80-C2-00-00</td>
<td>LLC-SNAP</td>
<td>00-00-0C-01</td>
<td>Bridge</td>
</tr>
</tbody>
</table>
Port Monitor Commands

30.1 port monitor

Use the port monitor Interface Configuration (Ethernet) mode command to start a port monitoring session (mirroring). Use the no form of this command to stop a port monitoring session.

Syntax

`port monitor src-interface-id [rx | tx]`
`no port monitor src-interface-id`
`port monitor vlan vlan-id`
`no port monitor vlan vlan-id`

Parameters

- **rx**—Monitors received packets only. If no option is specified, it monitors both rx and tx.
- **tx**—Monitors transmitted packets only. If no option is specified, it monitors both rx and tx.
- **vlan vlan-id**—VLAN number
- **src-interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

Default Configuration

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command enables port copy between Source Port (src-interface) to a Destination Port (The port in context).
The analyzer port for port ingress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for port egress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for VLAN mirroring should be the same for all the mirrored VLANs, and should be the same port as the analyzer port for port ingress mirroring traffic.

The following restriction applies to ports that are configured to be source ports:

- The port cannot be a destination port.

The following restrictions apply to ports that are configured to be monitor ports:

- The port cannot be source port.
- The port is not a member in port-channel.
- IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member in any VLAN, except for the default VLAN (will be automatically removed from the default VLAN).
- L2 protocols, such as: LLDP, CDP, LBD, STP, LACP, are not active on the destination port.

Notes:

1. 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 & 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).

2. When the port is configured to 802.1X auto mode it will forward any mirrored traffic regardless of the.1X state. However, it will operate as a normal network port (forward traffic) only after authorization is done.
3. Mirrored traffic is exposed to STP state, i.e. if the port is in STP blocking, it will not egress any mirrored traffic.

Example
The following example copies traffic for both directions (Tx and Rx) from the source port gi2 to destination port gi1.

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# port monitor gi2
```

### 30.2 show ports monitor

Use the `show ports monitor` EXEC mode command to display the port monitoring status.

Syntax

```
show ports monitor
```

Command Mode

EXEC mode

Example

The following example displays the port monitoring status.

```
switchxxxxxx# show ports monitor

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination Port</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi8</td>
<td>gi1</td>
<td>RX,TX</td>
<td>Active</td>
</tr>
<tr>
<td>gi2</td>
<td>gi1</td>
<td>RX,TX</td>
<td>Active</td>
</tr>
<tr>
<td>gi18</td>
<td>gi1</td>
<td>Rx</td>
<td>Active</td>
</tr>
<tr>
<td>VLAN 9</td>
<td>gi1</td>
<td>N/A</td>
<td>Active</td>
</tr>
</tbody>
</table>
```
31.1 spanning-tree

Use the `spanning-tree` Global Configuration mode command to enable spanning-tree functionality. Use the `no` form of this command to disable the spanning-tree functionality.

**Syntax**

```
spanning-tree
no spanning-tree
```

**Parameters**

N/A

**Default Configuration**

Spanning-tree is enabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables spanning-tree functionality.

```
switchxxxxxx(config)# spanning-tree
```

31.2 spanning-tree mode

Use the `spanning-tree mode` Global Configuration mode command to select which Spanning Tree Protocol (STP) protocol to run. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
spanning-tree mode {stp / rstp / mst}
```
no spanning-tree mode

Parameters

- **stp**—Specifies that STP is enabled.
- **rstp**—Specifies that the Rapid STP is enabled.
- **mst**—Specifies that the Multiple STP is enabled.

Default Configuration

The default is RSTP.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

The following example enables MSTP.

```
switchxxxxxx(config)# spanning-tree mode mstp
```

31.3 spanning-tree forward-time

Use the **spanning-tree forward-time** Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the **no** form of this command to restore the default configuration.

**Syntax**

- `spanning-tree forward-time seconds`
- `no spanning-tree forward-time`

---

**Notes:**

- **Parameters:**
  - **stp**
  - **rstp**
  - **mst**

- **Default Configuration:**
  - The default is RSTP.

- **Command Mode:**
  - Global Configuration mode

- **User Guidelines:**
  - RSTP mode: Uses STP when neighbor uses STP.
  - MSTP mode: Uses RSTP when neighbor uses RSTP; uses STP when neighbor uses STP.

- **Example:**
  - Enabling MSTP:
    ```
    switchxxxxxx(config)# spanning-tree mode mstp
    ```
Parameters
seconds—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration
15 seconds.

Command Mode
Global Configuration mode

User Guidelines
When configuring the forwarding time, the following relationship should be maintained:

\[ 2 \times (\text{Forward-Time} - 1) \geq \text{Max-Age} \]

Example
The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
switchxxxxxx(config)# spanning-tree forward-time 25
```

31.4 spanning-tree hello-time

Use the `spanning-tree hello-time` Global Configuration mode command to configure how often the device broadcasts Hello messages to other devices. Use the `no` form of this command to restore the default configuration.

Syntax
`spanning-tree hello-time seconds`
`no spanning-tree hello-time`

Parameters
seconds—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration
2 seconds.
Command Mode
Global Configuration mode

User Guidelines
When configuring the Hello time, the following relationship should be maintained:

\[ \text{Max-Age} \geq 2^*(\text{Hello-Time} + 1) \]

Example
The following example configures the spanning-tree bridge hello time to 5 seconds.

```
switchxxxxxx(config)# spanning-tree hello-time 5
```

31.5 spanning-tree max-age

Use the `spanning-tree max-age` Global Configuration mode command to configure the STP maximum age. Use the `no` form of this command to restore the default configuration.

Syntax
```
spanning-tree max-age seconds
no spanning-tree max-age
```

Parameters

- `seconds`—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration
The default maximum age is 20 seconds.

Command Mode
Global Configuration mode

User Guidelines
When configuring the maximum age, the following relationships should be maintained:
\[2^* (\text{Forward-Time} - 1) \geq \text{Max-Age}\]

\[\text{Max-Age} \geq 2^*(\text{Hello-Time} + 1)\]

### Example

The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
switchxxxxxx(config)# spanning-tree max-age 10
```

### 31.6 spanning-tree priority

Use the `spanning-tree priority` Global Configuration mode command to configure the device STP priority, which is used to determine which bridge is selected as the root bridge. Use the `no` form of this command to restore the default device spanning-tree priority.

**Syntax**

```
spanning-tree priority priority
no spanning-tree priority
```

**Parameters**

- **priority**—Specifies the bridge priority. (Range: 0–61440)

**Default Configuration**

Default priority = 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 spanning tree. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.
Example
The following example configures the spanning-tree priority to 12288.

```
switchxxxxxxx(config)# spanning-tree priority 12288
```

31.7 spanning-tree disable
Use the `spanning-tree disable` Interface Configuration (Ethernet, port-channel) mode command to disable the spanning tree on a specific port. Use the `no` form of this command to enable the spanning tree on a port.

Syntax
```
spanning-tree disable
no spanning-tree disable
```

Parameters
N/A

Default Configuration
Spanning tree is enabled on all ports.

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

Example
The following example disables the spanning tree on `gi5`

```
switchxxxxxxx(config)# interface gi5
switchxxxxxxx(config-if)# spanning-tree disable
```

31.8 spanning-tree cost
Use the `spanning-tree cost` Interface Configuration (Ethernet, port-channel) mode command to configure the spanning-tree path cost for a port. Use the `no` form of this command to restore the default configuration.
### Syntax

`spanning-tree cost cost`

`no spanning-tree cost`

#### Parameters

- **cost**: Specifies the port path cost. (Range: 1–200000000)

#### Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000 Mbps)</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

#### Command Mode

Interface Configuration (Ethernet, port-channel) mode

#### Example

The following example configures the spanning-tree cost on gi15 to 35000.

```
switchxxxxx(config)# interface gi15
switchxxxxx(config-if)# spanning-tree cost 35000
```

### 31.9 spanning-tree port-priority

Use the `spanning-tree port-priority` Interface Configuration (Ethernet, port-channel) mode command to configure the port priority. Use the `no` form of this command to restore the default configuration.

#### Syntax

- **spanning-tree port-priority priority**
- **no spanning-tree port-priority**
Parameters

**priority**—Specifies the port priority. (Range: 0–240)

**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 spanning priority on gi15 to 96

```
switchxxxxx(config)# interface gi15
switchxxxxx(config-if)# spanning-tree port-priority 96
```

31.10  spanning-tree portfast

Use the **spanning-tree portfast** Interface Configuration (Ethernet, port-channel) mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the **no** form of this command to disable the PortFast mode.

**Syntax**

```
spanning-tree portfast [auto]
no spanning-tree portfast
```

**Parameters**

**auto**—Specifies that the software waits for 3 seconds (with no Bridge Protocol Data Units (BPDUs) received on the interface) before putting the interface into the PortFast mode.
Default Configuration
PortFast mode is disabled.

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

Example
The following example enables the PortFast mode on gi15.

```
switchxxxxx(config)# interface gi15
switchxxxxx(config-if)# spanning-tree portfast
```

31.11 spanning-tree link-type

Use the `spanning-tree link-type` Interface Configuration (Ethernet, port-channel) mode command to override the default link-type setting determined by the port duplex mode, and enable RSTP transitions to the Forwarding state. Use the `no` form of this command to restore the default configuration.

Syntax

```
spanning-tree link-type {point-to-point | shared}
no spanning-tree 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 device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

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

The following example enables shared spanning-tree on gi15.

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# spanning-tree link-type shared
```

### 31.12 spanning-tree pathcost method

Use the `spanning-tree pathcost method` Global Configuration mode command to set the default path cost method. Use the `no` form of this command to return to the default configuration.

**Syntax**

```
spanning-tree pathcost method {long / short}
```

**no spanning-tree pathcost method**

**Parameters**

- `long`—Specifies that the default port path costs are within the range: 1–200,000,000.
- `short`—Specifies that the default port path costs are within the range: 1–65,535.

**Default Configuration**

Long path cost method.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command applies to all the spanning tree 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
```

31.13 spanning-tree bpdu (Global)

Use the `spanning-tree bpdu` Global Configuration mode command to define Bridge Protocol Data Unit (BPDU) handling when the spanning tree is disabled globally or on a single interface. Use the `no` form of this command to restore the default configuration.

Syntax
```
spanning-tree bpdu {filtering | flooding}
no spanning-tree bpdu
```

Parameters
- **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration
The default setting is flooding.

Command Mode
Global Configuration mode

User Guidelines
The filtering and flooding modes are relevant when the spanning tree is disabled globally or on a single interface.
Example

The following example defines the BPDU packet handling mode as flooding when the spanning tree is disabled on an interface.

switchxxxxxx(config)# spanning-tree bpdu flooding

31.14 spanning-tree bpdu (Interface)

Use the spanning-tree bpdu Interface Configuration (Ethernet, Port-channel) mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree bpdu [filtering | flooding]

no spanning-tree bpdu

Parameters

- filtering—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- flooding—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The spanning-tree bpdu (Global) command determines the default configuration.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example defines the BPDU packet as flooding when the spanning tree is disabled on gi3.

switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# spanning-tree bpdu flooding
31.15 spanning-tree guard root

use the `spanning-tree guard root` Interface Configuration (Ethernet, Port-channel) mode command to enable Root Guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the `no` form of this command to disable the root guard on the interface.

**Syntax**

```plaintext
spanning-tree guard root
no spanning-tree guard root
```

**Default Configuration**

Root guard is disabled.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

Root Guard can be enabled when the device operates in any mode (STP, RSTP and MSTP).

When Root Guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

**Example**

The following example prevents `gi 1` from being the root port of the device.

```plaintext
switchxxxxxx(config)# interface gi 1
switchxxxxxx(config-if)# spanning-tree guard root
```

31.16 spanning-tree bpduguard

Use the `spanning-tree bpduguard` Interface Configuration (Ethernet, port-channel) mode command to shut down an interface when it receives a Bridge Protocol Data Unit (BPDU). Use the `no` form of this command to restore the default configuration.
Syntax
spanning-tree bpdu-guard {enable | disable}
no spanning-tree bpdu-guard

Parameters
bpdu-guard enable—Enables BPDU Guard.
bpdu-guard disable—Disables BPDU Guard.

Default Configuration
BPDU Guard is disabled.

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

User Guidelines
The command can be enabled when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

Example
The following example shuts down gi5 when it receives a BPDU.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# spanning-tree bpdu-guard enable
```

31.17 clear spanning-tree detected-protocols

Use the clear spanning-tree detected-protocols Privileged EXEC command to restart the STP migration process (force renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

```
clear spanning-tree detected-protocols [interface interface-id]
```
Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This feature can only be used when working in RSTP or MSTP mode.

Example

This restarts the STP migration process on all interfaces.

```
switchxxxxxx# clear spanning-tree detected-protocols
```

### 31.18 spanning-tree mst priority

Use the `spanning-tree mst priority` Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
spanning-tree mst instance-id priority priority
no spanning-tree mst instance-id priority
```

**Parameters**

- **instance-id**—Specifies the spanning-tree instance ID. (Range: 1–15)
- **priority**—Specifies the device priority for the specified spanning-tree instance. This setting determines the likelihood 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: 0–61440)
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 spanning tree.

Example
The following example configures the spanning tree priority of instance 1 to 4096.

```
switchxxxxxx(config)# spanning-tree mst 1 priority 4096
```

31.19 spanning-tree mst max-hops

Use the `spanning-tree mst max-hops` Global Configuration mode command to configure the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the `no` form of this command to restore the default configuration.

Syntax
```
spanning-tree mst max-hops hop-count
no spanning-tree mst max-hops
```

Parameters
`max-hops hop-count`—Specifies the number of hops in an MST region before the BDPU is discarded. (Range: 1–40)

Default Configuration
The default number of hops is 20.

Command Mode
Global Configuration mode
Example
The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
switchxxxxxx(config)# spanning-tree mst max-hops 10
```

31.20 spanning-tree mst port-priority
Use the spanning-tree mst port-priority Interface Configuration (Ethernet, port-channel) mode command to configure the priority of a port. Use the no form of this command to restore the default configuration.

Syntax
```
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

Parameters
- `instance-id`—Specifies the spanning tree instance ID. (Range: 1–15)
- `priority`—Specifies the port priority. (Range: 0–240 in multiples of 16)

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
```
31.21 spanning-tree mst cost

Use the spanning-tree mst cost Interface Configuration (Ethernet, Port-channel) mode command to configure the path cost for MST calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the Forwarding state. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree mst instance-id cost cost

no spanning-tree mst instance-id cost

Default Configuration

N/A

Parameters

- instance-id—Specifies the spanning-tree instance ID. (Range: 1–15)
- cost—Specifies the port path cost. (Range: 1–200000000)

Default Configuration

Default path cost is determined by the port speed and path cost method (long or short) as shown below:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000 Mbps)</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example configures the MSTP instance 1 path cost for gigabitethernet port 9 to 4.

switchxxxxxx(config)# interface gi9
31.22 spanning-tree mst configuration

Use the `spanning-tree mst configuration` Global Configuration mode command to enable configuring an MST region by entering the MST mode.

**Syntax**

```
spanning-tree mst configuration
```

**Command Mode**

Global Configuration mode

**User Guidelines**

For two or more switches to be in the same MST region, they must contain the same VLAN mapping, the same configuration revision number, and the same name.

**Example**

The following example configures an MST region.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
switchxxxxxx(config-mst)# name region1
switchxxxxxx(config-mst)# revision 1
```

31.23 instance (MST)

Use `instance` MST Configuration mode command to map VLANs to an MST instance. Use the `no` form of this command to restore the default mapping.

**Syntax**

```
instance instance-id vlan vlan-range
no instance instance-id vlan vlan-range
```
Parameters

- **instance-id**—MST instance (Range: 1–15)

- **vlan-range**—The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1–4094)

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 MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
```

31.24 name (MST)

Use the **name** MST Configuration mode command to define the MST instance name. Use the **no** form of this command to restore the default setting.

Syntax

```
name string
no name
```
Parameters

string—Specifies the MST instance name. (Length: 1–32 characters)

Default Configuration

The default name is the bridge MAC address.

Command Mode

MST Configuration mode

Example

The following example defines the instance name as Region1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

31.25 revision (MST)

Use the revision MST Configuration mode command to define the MST configuration revision number. Use the no form of this command to restore the default configuration.

Syntax

```
revision value

no revision
```

Parameters

value—Specifies the MST configuration revision number. (Range: 0–65535)

Default Configuration

The default configuration revision number is 0.

Command Mode

MST Configuration mode
Example
The following example sets the configuration revision to 1.

```
switchxxxxxx(config) # spanning-tree mst configuration
switchxxxxxx(config-mst) # revision 1
```

31.26 show (MST)
Use the show MST Configuration mode command to display the current or pending MST region configuration.

Syntax
```
show {current | pending}
```

Parameters
- **current**—Displays the current MST region configuration.
- **pending**—Displays the pending MST region configuration.

Default Configuration
N/A

Command Mode
MST Configuration mode

Example
The following example displays a pending MST region configuration

```
switchxxxxxx(config-mst)# show pending
Gathering information .......... 
Current MST configuration 
Name: Region1
Revision: 1
Instance  VLANs Mapped State
--------  ------------------------  -----
```
31.27 exit (MST)

Use the `exit` MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

**Syntax**

`exit`

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

MST Configuration mode

**Example**

The following example exits the MST Configuration mode and saves changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# exit
switchxxxxxx(config)#
```
Parameters
N/A

Default Configuration
N/A

Command Mode
MST Configuration mode

Example
The following example exits the MST Configuration mode without saving changes.

switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# abort

31.29 show spanning-tree
Use the show spanning-tree Privileged EXEC mode command to display the spanning-tree configuration.

Syntax
show spanning-tree [interface-id] [instance instance-id]
show spanning-tree [detail] [active / blockedports] [instance instance-id]
show spanning-tree mst-configuration

Parameters
- instance instance-id—Specifies the spanning tree instance ID. (Range: 1–15)
- detail—Displays detailed information.
- active—Displays active ports only.
- blockedports—Displays blocked ports only.
- mst-configuration—Displays the MST configuration identifier.
- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
Default Configuration

If no interface is specified, the default is all interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This command only works when MST is enabled.

Example

The following examples display spanning-tree information in various configurations:

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID  Priority  32768
         Address  00:01:42:97:e0:00
         Cost  20000
         Port  gi1
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority  36864
          Address  00:02:4b:29:7a:00
          Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```
Spanning Tree Commands

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio. No</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>gi2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td></td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID | Priority | Address
--------|----------|-----------------
36864   | 00:02:4b:29:7a:00
This switch is the Root.

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio. Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>gi2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>gi5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td></td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

Root ID | Priority | Address
--------|----------|-----------------
N/A     | N/A      | N/A             |
Path Cost | N/A      | Root Port N/A     |
Hello Time | N/A      | Max Age N/A     Forward Delay N/A

Bridge ID | Priority | Address
---------|----------|-----------------
36864   | 00:02:4b:29:7a:00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Spanning-Tree Commands

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFastType</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>gi5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

```
switchxxxxxx# show spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID   Priority 32768
          Address 00:01:42:97:e0:00
          Path Cost 20000
          Root Port gi1
          Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 36864
          Address 00:02:4b:29:7a:00
          Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFastType</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>gi2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No Shared (STP)</td>
</tr>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No Shared (STP)</td>
</tr>
</tbody>
</table>

```
switchxxxxxx# show spanning-tree blockedports
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID   Priority 32768
          Address 00:01:42:97:e0:00
          Path Cost 20000
          Root Port gi1
          Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```
Spanning-Tree Commands

Bridge ID  Priority  36864
  Address  00:02:4b:29:7a:00
  Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>19</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree detail
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID  Priority  32768
  Address  00:01:42:97:e0:00
  Path Cost  20000
  Root Port  gi1
  Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority  36864
  Address  00:02:4b:29:7a:00
  Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 2d18h ago
Times:  hold 1, topology change 35, notification 2
  hello 2, max age 20, forward delay 15

Port 1 (gi1) enabled
State: Forwarding  Role: Root
Port id: 128.1  Port cost: 20000
Type: P2p (configured: auto) RSTP  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:01:42:97:e0:00
Designated port id: 128.25  Designated path cost: 0
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Role</th>
<th>Port ID</th>
<th>Type</th>
<th>Designated Bridge Priority</th>
<th>Designated Port ID</th>
<th>Guard Root</th>
<th>Port Cost</th>
<th>Port Fast</th>
<th>Address</th>
<th>Designated Path Cost</th>
<th>BPDU Guard</th>
<th>Number of Transitions</th>
<th>BPDU Sent</th>
<th>BPDU Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (gi2) enabled</td>
<td>Forwarding</td>
<td>Designated</td>
<td>128.2</td>
<td>Shared (configured: auto) STP</td>
<td>32768</td>
<td>128.2</td>
<td>Disabled</td>
<td>20000</td>
<td>No (configured: no)</td>
<td>00:02:4b:29:7a:00</td>
<td>20000</td>
<td>Disabled</td>
<td>1</td>
<td>2</td>
<td>170638</td>
</tr>
<tr>
<td>3 (gi3) disabled</td>
<td>N/A</td>
<td>N/A</td>
<td>128.3</td>
<td>N/A (configured: auto)</td>
<td>N/A</td>
<td>N/A</td>
<td>Disabled</td>
<td>20000</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Disabled</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>4 (gi4) enabled</td>
<td>Blocking</td>
<td>Alternate</td>
<td>128.4</td>
<td>Shared (configured: auto) STP</td>
<td>28672</td>
<td>128.25</td>
<td>Disabled</td>
<td>20000</td>
<td>No (configured: no)</td>
<td>00:30:94:41:62:c8</td>
<td>20000</td>
<td>Disabled</td>
<td>1</td>
<td>2</td>
<td>120638</td>
</tr>
<tr>
<td>5 (gi5) enabled</td>
<td>Disabled</td>
<td>N/A</td>
<td>128.5</td>
<td>N/A (configured: auto)</td>
<td>N/A</td>
<td>N/A</td>
<td>Disabled</td>
<td>20000</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Disabled</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
switchxxxxxx# show spanning-tree ethernet gi1
Port 1 (gi1) enabled
State: Forwarding Role: Root
Port id: 128.1 Port cost: 20000
Type: P2p (configured: auto) RSTP Port Fast: No (configured: no)
Designated bridge Priority: 32768 Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

switchxxxxxx# show spanning-tree mst-configuration
Name: Region1
Revision: 1

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-9, 21-4094</td>
<td>Enabled</td>
</tr>
<tr>
<td>1</td>
<td>10-20</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
##### MST 0 Vlans Mapped: 1-9

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
<th>Max hops</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:01:42:97:e0:00</td>
<td>20000</td>
<td>gi1</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>Address</th>
<th>This switch is the IST master.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:02:4b:29:7a:00</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
<th>Max hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
<td></td>
</tr>
</tbody>
</table>

Interfaces
### Spanning Tree Commands

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
</tr>
<tr>
<td>gi2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>gi3</td>
<td>Enabled</td>
<td>128.3</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
</tr>
</tbody>
</table>

### MST 1 Vlans Mapped: 10-20

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi4</td>
<td>20000</td>
<td>00:02:4b:29:89:76</td>
<td>24576</td>
<td></td>
</tr>
</tbody>
</table>

### Bridge ID

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>Address</th>
<th>Rem hops</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:02:4b:29:7a:00</td>
<td>19</td>
</tr>
</tbody>
</table>

### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Boun</td>
<td>No</td>
</tr>
<tr>
<td>gi2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Boun</td>
<td>No</td>
</tr>
<tr>
<td>gi3</td>
<td>Enabled</td>
<td>128.3</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
</tr>
<tr>
<td>gi4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
</tr>
</tbody>
</table>

### Switch Configuration

```
switchxxxxxx# show spanning-tree detail
Spanning tree enabled mode MSTP
Default port cost method: long
```

### MST 0 Vlans Mapped: 1-9

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>32768</td>
<td>00:01:42:97:e0:00</td>
<td>20000</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:02:4b:29:7a:00</td>
</tr>
</tbody>
</table>
This switch is the IST master.
Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec
Max hops 20
Number of topology changes 2 last change occurred 2d18h ago
Times:  hold 1, topology change 35, notification 2
      hello 2, max age 20, forward delay 15

Port 1 (gi1) enabled
State: Forwarding  Role: Root
Port id: 128.1  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP  Port Fast: No (configured: no)
Designated bridge Priority: 32768  Address: 00:01:42:97:e0:00
Designated port id: 128.25  Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (gi2) enabled
State: Forwarding  Role: Designated
Port id: 128.2  Port cost: 20000
Type: Shared (configured: auto) Boundary STP  Port Fast: No (configured: no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (gi3) enabled
State: Forwarding  Role: Designated
Port id: 128.3  Port cost: 20000
Type: Shared (configured: auto) Internal  Port Fast: No (configured: no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.3  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
Port 4 (gi4) enabled
State: Forwarding  Role: Designated
Port id: 128.4  Port cost: 20000
Type: Shared (configured: auto) Internal  Port Fast: No (configured: no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

#### MST 1 Vlans Mapped: 10-20

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>24576</td>
<td>00:02:4b:29:89:76</td>
<td>20000</td>
<td>gi4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rem hops 19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>Address</th>
<th>Number of topology changes 2 last change occurred 1d9h ago</th>
<th>Times: hold 1, topology change 2, notification 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:02:4b:29:7a:00</td>
<td></td>
<td>hello 2, max age 20, forward delay 15</td>
</tr>
</tbody>
</table>

Port 1 (gi1) enabled
State: Forwarding  Role: Boundary
Port id: 128.1  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP  Port Fast: No (configured: no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.1  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
Port 2 (gi2) enabled
State: Forwarding     Role: Designated
Port id: 128.2        Port cost: 20000
Type: Shared (configured: auto) Boundary STP Port Fast: No (configured:no)
Designated bridge Priority: 32768      Address: 00:02:4b:29:7a:00
Designated port id: 128.2     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (gi3) disabled
State: Blocking       Role: Alternate
Port id: 128.3        Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768      Address: 00:02:4b:29:1a:19
Designated port id: 128.78     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (gi4) enabled
State: Forwarding     Role: Designated
Port id: 128.4        Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768      Address: 00:02:4b:29:7a:00
Designated port id: 128.2     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
#### MST 0 Vlans Mapped: 1-9
CST Root ID     Priority 32768
               Address 00:01:42:97:e0:00
               Path Cost 20000
               Root Port gi1
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
31.30  show spanning-tree bpdu

Use the show spanning-tree bpdu EXEC mode command to display the BPDU handling when spanning-tree is disabled.

Syntax

show spanning-tree bpdu [interface-id | detailed]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.
Default Configuration

Show information for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following examples display spanning-tree BPDU information:

switchxxxxxxx# show spanning-tree bpdu

The following is the output if the global BPDU handling command is not supported.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Filtering</td>
<td>Filtering</td>
</tr>
<tr>
<td>gi2</td>
<td>Filtering</td>
<td>Filtering</td>
</tr>
<tr>
<td>gi3</td>
<td>Filtering</td>
<td>Guard</td>
</tr>
</tbody>
</table>

The following is the output if both the global BPDU handling command and the per-interface BPDU handling command are supported.

Global: Flooding

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Global</td>
<td>Flooding</td>
</tr>
<tr>
<td>gi2</td>
<td>Global</td>
<td>STP</td>
</tr>
<tr>
<td>gi3</td>
<td>Flooding</td>
<td>STP</td>
</tr>
</tbody>
</table>
32.1 vlan database

Use the `vlan database` Global Configuration mode command to enter the VLAN Configuration mode. This mode is used to create VLAN(s) and define the default VLAN.

Use the `exit` command to return to Global Configuration mode.

Syntax

`vlan database`

Parameters

N/A

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

Example

The following example enters the VLAN Configuration mode, creates VLAN 1972 and exits VLAN Configuration mode.

```bash
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 1972
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)#
```
32.2 vlan

Use the `vlan` VLAN Configuration mode command to create a VLAN. Use the `no` form of this command to delete the VLAN(s).

To assign the VLAN a name, use the Interface Configuration (VLAN) mode `name` command.

**Syntax**

`vlan vlan-range`

`no vlan vlan-range`

**Parameters**

- `vlan-range`—Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 2-4094).

**Default Configuration**

VLAN 1 exists by default.

**Command Mode**

VLAN Configuration mode

**Example**

The following example creates VLANs 100 and 1972.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 100,1972
switchxxxxxx(config-vlan)#
```

32.3 show vlan

Use the `show vlan` Privileged EXEC mode command to display the following VLAN information for all VLANs or for a specific VLAN:

- VLAN ID
- VLAN name
- Ports on the VLAN
- Whether the VLAN was is dynamic or permanent
- Whether authorization is required on the VLAN

**Syntax**

```bash
show vlan [tag vlan-id | name vlan-name]
```

**Parameters**

- `tag vlan-id`—Specifies a VLAN ID.
- `name vlan-name`—Specifies a VLAN name string (length: 1–32 characters)

**Default Configuration**

All VLANs are displayed.

**Command Mode**

Privileged EXEC mode
Examples

Example 1 - The following example displays information for all VLANs.

```
switchxxxxxx# show vlan

VLAN  Name      Ports   Type    Authorization
-----  --------   -------   ------   ------------
    1 default    gi1-2   Default  Required
   10 Marketing  gi3-14  Static   Required
   11      11      gi5-16  Static   Required
   20      20      gi7-18  Static   Required
   21      21      gi7     Static   Required
   30      30      gi7     Static   Required
   31      31      gi7     Static   Required
   91      91      gi2     Dynamic Not Required
  3978    Guest VLAN gi7     Static   Guest
```

Example 2 - The following example displays information for the default VLAN (VLAN 1):

```
switchxxxxxx# show vlan tag default

VLAN  Name      Ports   Type    Authorization
-----  --------   -------   ------   ------------
    1 default    gi1-2   Default  Required
```
Example 3 - The following example displays information for the VLAN named Marketing:

```
switchxxxxxx# show vlan name Marketing

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Marketing</td>
<td>gi3-14</td>
<td>static</td>
<td>Required</td>
</tr>
</tbody>
</table>
```

32.4  default-vlan vlan

Use the `default-vlan vlan` VLAN Configuration mode command to define the default VLAN. Use the `no` form of this command to set VLAN 1 as the default VLAN.

Syntax

default-vlan vlan `vlan-id`

no default-vlan vlan

Parameters

`vlan vlan-id`—Specifies the default VLAN ID.

Default Configuration

The default VLAN is 1 by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command becomes effective after reboot of the device.

Example

The following example defines the default VLAN as 2.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# default-vlan vlan 2
```
New Default VLAN ID will be active after save configuration and reboot device.

32.5  **show default-vlan-membership**

Use the `show default-vlan-membership` privileged EXEC command to view the default VLAN membership.

**Syntax**

```plaintext
show default-vlan-membership [interface-id | detailed]
```

**Parameters**

- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- `detailed`—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Membership in the default VLAN is displayed for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

Privileged EXEC

**Example**

```
switchxxxxxx # show default-vlan-membership
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Forbidden</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>gi2</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>gi3</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

32.6  **interface vlan**

Use the `interface vlan` Global Configuration mode command to enter the Interface Configuration (VLAN) mode for a specific VLAN. After this command is entered, all commands configure this VLAN. To configure a range of VLANs, use `interface range vlan`. 


Syntax

interface vlan vlan-id

Parameters

vlan vlan-id—Specifies the VLAN to be configured.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

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

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

32.7 interface range vlan

Use the interface range vlan Global Configuration mode command to configure multiple VLANs simultaneously.

Syntax

interface range vlan vlan-range

Parameters

vlan vlan-range—Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

Default Configuration

N/A

Command Mode

Global Configuration mode
User Guidelines

Commands under the interface VLAN range context are executed independently on each VLAN in the range. If the command returns an error on one of the VLANs, an error message is displayed, and the system attempts to configure the remaining VLANs.

Example

The following example groups VLANs 221 through 228 and 889 to receive the same command(s).

```
switchxxxxxx(config)# interface range vlan 221-228, vlan 889
switchxxxxxx(config-if)#
```

32.8 name

Use the name Interface Configuration (VLAN) mode command to name a VLAN. Use the no form of this command to remove the VLAN name.

Syntax

name string

no name

Parameters

string—Specifies a unique name associated with this VLAN. (Length: 1–32 characters)

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

The VLAN name must be unique.
Example
The following example assigns VLAN 19 the name Marketing.

switchxxxxxx(config)# interface vlan 19
switchxxxxxx(config-if)# name Marketing

32.9 switchport protected-port

Use the switchport protected-port Interface Configuration mode command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports on the same switch. Use the no form of this command to disable protection on the port.

Syntax
switchport protected-port
no switchport protected-port

Parameters
N/A

Default Configuration
Unprotected

Command Mode
Interface configuration (Ethernet, port-channel)

User Guidelines
Note that packets are subject to all filtering rules and Filtering Database (FDB) decisions.

Example

switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport protected-port
32.10  show interfaces protected-ports

Use the show interfaces protected-ports EXEC mode command to display protected ports configuration.

Syntax

show interfaces protected-ports [interface-id | detailed]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Show all protected interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

```
switchxxxxxx# show interfaces protected-ports
Interface     State
--------- -------------
   gi1      Protected
   gi2      Protected
   gi3      Unprotected
   gi4      Unprotected
```

32.11  switchport mode

Use the switchport mode Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN membership mode (access, trunk, general or
customer) of a port. Use the no form of this command to restore the default configuration.

Syntax

switchport mode {access / trunk / general / customer}

no switchport mode

Parameters

- **access**—Specifies an untagged layer 2 VLAN port.
- **trunk**—Specifies a trunking layer 2 VLAN port.
- **general**—Specifies a full 802-1q-supported VLAN port.
- **customer**—Specifies that the port is connected to customer equipment. Used when the switch is in a provider network.

Default Configuration

Trunk mode.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- When the port’s mode is changed, it receives the configuration corresponding to the mode.
- If the port mode is changed to access and the access VLAN does not exist, then the port does not belong to any VLAN.
- Trunk and general mode 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 (untagged layer 2) VLAN port.

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport mode access
```
32.12 switchport access vlan

An interface in access mode can belong to only one VLAN. Use the **switchport access vlan** Interface Configuration command to reassign an interface to a different VLAN than it currently belongs to.

Use the **no** form of this command to restore the default configuration.

**Syntax**

```
switchport access vlan vlan-id
no switchport access vlan
```

**Parameters**

- **vlan vlan-id**—Specifies 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 the specified VLAN.

If the interface is a forbidden member of the specified VLAN, it does not become a member of the VLAN. An error message is displayed ("An interface cannot become a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute if there are more interfaces in the interface list.

**Examples**

**Example 1**—The following example sets 152 as an access port and assigns it to VLAN 2 (and removes it from its previous VLAN).

```
switchxxxxxxx(config-if)# switchport access vlan 2
```
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2

switchxxxxxx#show vlan

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>gi1-28,Po1-8</td>
<td>Default</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Example 2**—The following example shows a case where a macro is defined that adds ports to VLANs. Some of the ports are forbidden members in some of the VLANs. The example shows that the system notifies the user that it cannot add the forbidden ports, but does not fail the macro and it continues to a normal end.

switchxxxxxx# configure
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 2-5
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface range 151-2
switchxxxxxx(config-if-range)# switchport forbidden vlan add 2-3
switchxxxxxx(config-if-range)# exit
switch345780(config)#
switch345780(config)# macro name Trunk_VLAN
Enter macro commands one per line. End with the character '@'.
switchport mode trunk
switchport trunk allowed vlan add $1stVLAN-$2ndVLAN
@
switchxxxxxx(config)# interface range 151-4
switchxxxxxx(config-if-range)# macro apply Trunk_VLAN $1stVLAN 2 $2ndVLAN 5
An interface cannot become a member of a forbidden VLAN <System notifies user that an illegal action has been requested but continues executing the macro>
switchxxxxxx(config-if-range)# end
switchxxxxxx#show vlan
<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>151-28, Po1-8</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>153-4</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>153-4</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>151-4</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>151-4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 32.13 switchport trunk allowed vlan

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. Use the `switchport trunk allowed vlan` Interface Configuration mode command to add/remove VLAN(s) to/from a trunk port.

**Syntax**

`switchport trunk allowed vlan {add vlan-list | remove vlan-list}`

**Parameters**

- `add vlan-list` — Specifies a list of VLAN IDs to add to a port. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- `remove vlan-list` — Specifies a list of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

**Default Configuration**

By default, trunk ports belongs to all created VLANs.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

If the interface is a forbidden member of the specified VLAN, it does not become a member of the VLAN. An error message is displayed. An interface cannot become a member of a forbidden VLAN. This message will only be displayed
once.

and the command continues to execute if there are more VLANs in the VLAN list. See the example in switchport access vlan.

Example

To add VLANs 2,3 and 100 to trunk ports 1 to 13:

```
switchxxxxxx(config)# interface range 151-13
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
```

32.14 switchport trunk native vlan

If an untagged packet arrives on a trunk port, it is directed to the port’s native VLAN. Use the switchport trunk native vlan Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN for a trunk interface. Use the no form of this command to restore the default native VLAN.

Syntax

```
switchport trunk native vlan vlan-id
no switchport trunk native vlan
```

Parameters

- **vlan-id**— Specifies 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 the VLAN.

If the interface is a forbidden member of the specified VLAN, it does not become a member of the VLAN, but the command does not fail. Instead, an error message is
displayed ("An interface cannot become a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute if there are more VLANs in the VLAN list. See the example in `switchport access vlan`.

**Examples**

**Example 1**—The following example:

- Defines VLAN 2 as native VLAN for port 1
- Removes VLAN 2 from port 1 and then sets it as the native VLAN

```
switchxxxxxx(config)# interface 151
switchxxxxxx(config-if)# switchport trunk native vlan 2
Port 1: Port is Trunk in VLAN 2.
switchxxxxxx(config-if)# switchport trunk allowed vlan remove 2
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)#
```

**Example 2**—The following example sets packets on port as untagged on ingress and untagged on egress:

```
switchxxxxxx(config)# interface 151
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)#
```

**Example 3**—The following example sets packets on port as tagged on ingress and tagged on egress:

```
switchxxxxxx(config)# interface 151
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2
switchxxxxxx(config-if)#
```
32.15 switchport general allowed vlan

General ports can receive tagged or untagged packets. Use the `switchport general allowed vlan` Interface Configuration mode command to add/remove VLANs to/from a general port and configure whether packets on the egress are tagged or untagged.

Use the `no` form of this command to reset to the default.

**Syntax**

```
switchport general allowed vlan {[add vlan-list [tagged | untagged]] | [remove vlan-list]}
```

**Parameters**

- `add vlan-list`—Specifies the list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

- `tagged`—Specifies that the port transmits tagged packets for the VLANs. This is the default value

- `untagged`—Specifies that the port transmits untagged packets for the VLANs.

- `remove vlan-list`—Specifies the list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

**Default Configuration**

The port is not member in any VLAN.

Packets are transmitted 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.

If the interface is a forbidden member of the specified VLAN, it does not become a member of the VLAN, but the command does not fail. Instead, an error message is displayed ('An interface cannot become a member of a forbidden VLAN. This
message will only be displayed once,”) and the command continues to execute if there are more VLANs in the VLAN list. See the example in switchport access vlan.

Example
Sets port 1 to general mode and adds VLAN 2 and 3 to it. Packets are tagged on the egress.

switchxxxxxx(config)# interface 151
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged

32.16 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. Use the switchport general pvid Interface Configuration (Ethernet, Port-channel) mode command to configure the Port VLAN ID (PVID) of an interface when it is in general mode. Use the no form of this command to restore the default configuration.

Syntax
switchport general pvid vlan-id
no switchport general pvid

Parameters
pvid vlan-id—Specifies the Port VLAN ID (PVID).

Default Configuration
The default VLAN is the PVID.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode
Examples

Example 1 - The following example configures port 2 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 - Performs the following:

- Adds VLANs 2&3 as tagged, and VLAN 100 as untagged to general mode port 14
- Defines VID 100 as the PVID
- 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 2-3 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
switchxxxxxx(config-if)#
```

Example 3 - Configures VLAN on port 14 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
switchxxxxxx(config-if)#
```
Example 4 - Configures VLAN on port 21 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 - Configures VLAN on port 14 as tagged on input and tagged on output:

```
switchxxxxxx(config)# interface gi14
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
```

Example 6 - Configures VLAN on port 23 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
```

32.17 switchport general ingress-filtering disable

Use the `switchport general ingress-filtering disable` Interface Configuration (Ethernet, Port-channel) mode command to disable port ingress filtering (no packets are discarded at the ingress) on a general port. Use the no form of this command to restore the default configuration.

**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.

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

32.18 switchport general acceptable-frame-type

The `switchport general acceptable-frame-type` Interface Configuration mode command configures the types of packets (tagged/untagged) that are filtered (discarded) on the interface. Use the `no` form of this command to return ingress filtering to the default.

Syntax

```
switchport general acceptable-frame-type {tagged-only | untagged-only | all}
no switchport general acceptable-frame-type
```

Parameters

- tagged-only—Ignore (discard) untagged packets and priority-tagged packets.
- untagged-only—Ignore (discard) VLAN-tagged packets (not including priority-tagged packets)
- all—Do 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 port gi3 to be in general mode and to discard untagged frames at ingress.

```
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type tagged-only
```

### 32.19 switchport customer vlan

When a port is in customer mode it is in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across a provider network. The switch is in QinQ mode when it has one or more customer ports.

Use the `switchport customer vlan` Interface Configuration mode command to set the port's VLAN when the interface is in customer mode (set by `switchport mode`). Use the no form of this command to restore the default configuration.

**Syntax**
```
switchport customer vlan vlan-id
no switchport customer vlan
```

**Parameters**
- `vlan vlan-id`—Specifies the customer VLAN.

**Default Configuration**
No VLAN is configured as customer.

**Command Mode**
Interface Configuration (Ethernet, Port-channel) mode
Example
The following example defines gi5 as a member of customer VLAN 5.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

### 32.20 map mac macs-group

Forwarding of packets based on their MAC address requires setting up groups of MAC addresses and then mapping these groups to VLANs.

Use the `map mac macs-group` VLAN Configuration mode command to map a MAC address or range of MAC addresses to a group of MAC addresses, which is then used in `switchport general map macs-group vlan`. Use the `no` form of this command to delete the mapping.

This command can only be used when the device is in Layer 2 mode.

**Syntax**

```
map mac mac-address {prefix-mask / host} macs-group group
no map mac mac-address {prefix-mask / host}
```

**Parameters**

- `mac mac-address`—Specifies the MAC address to be mapped to the group of MAC addresses.
- `prefix-mask`—Specifies the number of ones in the mask.
- `host`—Specifies that the mask is comprised of all 1s.
- `macs-group group`—Specifies the group number (range: 1–2147483647)

**Default Configuration**

N/A

**Command Mode**

VLAN Configuration mode
Example
The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface gill
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3

32.21 switchport general map macs-group vlan
After groups of MAC addresses have been created (see map mac macs-group), they can be mapped to specific VLANs.

Use the switchport general map macs-group vlan Interface Configuration (Ethernet, Port-channel) mode command to set a MAC-based classification rule. Use the no form of this command to delete a classification rule.

Syntax
switchport general map macs-group group vlan vlan-id
no switchport general map macs-group group

Parameters
- macs-group group—Specifies the group number (range: 1–2147483647)
- vlan vlan-id—Defines the VLAN ID associated with the rule.

Default Configuration
N/A

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

MAC-based VLAN rules cannot contain overlapping ranges on the same interface.

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules).
   1. Subnet-based VLAN (Best match among the rules).
   2. Protocol-based VLAN.
   3. PVID.

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface gi11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

32.22 show vlan macs-groups

Use the `show vlan macs-groups` EXEC mode command to display the MAC addresses that belong to the defined MACs-groups.

Syntax

`show vlan macs-groups`

Parameters

- N/A

Default Configuration

- N/A
Virtual Local Area Network (VLAN) Commands

32

Command Mode
EXEC mode

Example
The following example displays macs-groups information.

```
switchxxxxxx# show vlan macs-groups

+---------------------+---------------------+---------------------+
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Mask</th>
<th>Group ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:12:34:56:78:90</td>
<td>20</td>
<td>22</td>
</tr>
<tr>
<td>00:60:70:4c:73:ff</td>
<td>40</td>
<td>1</td>
</tr>
</tbody>
</table>
```

32.23 switchport forbidden default-vlan

Use the `switchport forbidden default-vlan` Interface Configuration command to forbid a port from being added to the default VLAN. Use the no form of this command to revert to default.

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)

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 conditions are met.

**Example**

The following example forbids the port gi1 from being added to the default VLAN.

```plaintext
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)# switchport forbidden default-vlan
```

### 32.24 `switchport forbidden vlan`

The `switchport forbidden vlan` Interface Configuration (Ethernet, Port-channel) mode command forbids adding or removing specific VLANs to or from a port. To restore the default configuration, use the `no` form of this command.

**Syntax**

```plaintext
switchport forbidden vlan [add vlan-list | remove vlan-list]
no switchport forbidden vlan [add vlan-list | remove vlan-list]
```

**Parameters**

- `add vlan-list` — Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen designate a range of IDs.

- `remove vlan-list` — Specifies a list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen designate a range of IDs.

**Default Configuration**

All VLANs are allowed.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode
Example
The following example forbids adding VLAN IDs 234 to 256 to gi7.

```
switchxxxxxx(config)# interface gi7
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport forbidden vlan add 234-256
```

### 32.25 `switchport default-vlan tagged`

Use the `switchport default-vlan tagged` Interface Configuration command to configure the port as a tagged port in the default VLAN. Use the `no` form of the command to return the port to an untagged port.

#### Syntax
```
switchport default-vlan tagged
no switchport default-vlan tagged
```

#### Parameters

**default-vlan tagged**

N/A

#### Default Configuration

If the port is a member in the default VLAN, by default, it is a member as an untagged port.

#### Command Mode

Interface configuration (Ethernet, port-channel)

#### 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.

Note:

- 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 the port gi1 as a tagged port in the default VLAN.

```
switchxxxxxxx(config)#interface gi1
switchxxxxxxx(config-if)# switchport mode trunk
switchxxxxxxx(config-if)#switchport default-vlan tagged
```
32.26 show interfaces switchport

Use the `show interfaces switchport` Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

**Syntax**

`show interfaces switchport [interface-id]`

**Parameters**

`interface-id`—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Default Configuration**

Displays information for all interfaces.

**Command Mode**

EXEC mode

**Examples**

**Example 1** - The following example displays the command output for a trunk port:

```
switchxxxxxx# show interfaces switchport gi1

Port gi1:
Port Mode: Trunk
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 2
Protected: Enabled, Uplink is gi9.
Port gi1 is member in:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>untagged</td>
<td>System</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>tagged</td>
<td>Dynamic</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>tagged</td>
<td>Static</td>
</tr>
</tbody>
</table>
```
Forbidden VLANS:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>Out</td>
</tr>
</tbody>
</table>

Classification rules:

Mac based VLANs:

Group ID  Vlan ID

---  -------

Example 2 - The following example displays the output for a general port:

```
switchxxxxxx# show interfaces switchport gi2
```

Port gi2:

VLAN Membership mode: General

Operating Parameters:

PVID: 4095 (discard vlan)

Ingress Filtering: Enabled

Acceptable Frame Type: All

GVRP status: Enabled

Protected: Disabled

Port gi1 is member in:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>IP Telephony</td>
<td>tagged</td>
</tr>
</tbody>
</table>

Protected: Disabled

Port gi2 is statically configured to:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>72</td>
<td>untagged</td>
</tr>
<tr>
<td>91</td>
<td>IP Telephony</td>
<td>tagged</td>
</tr>
</tbody>
</table>

Forbidden VLANS:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example 3 - The following example displays the command output for an access port:

```
switchxxxxx# show interfaces switchport gi2
Port gi2:
  Port Mode: Access
  Gvrp Status: disabled
  Ingress Filtering: true
  Acceptable Frame Type: admitAll
  Ingress UnTagged VLAN ( NATIVE ): 1
Port is member in:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Port Membership</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Untagged</td>
<td>System</td>
<td></td>
</tr>
</tbody>
</table>

Forbidden VLANS:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Name</th>
</tr>
</thead>
</table>

Classification rules:

Mac based VLANS:
```

### 32.27 ip internal-usage-vlan

The system assigns a VLAN to every IP address. In rare cases, this might conflict with a user requirement for that VLAN. In this case, use the `ip internal-usage-vlan` Interface Configuration (Ethernet, Port-channel) mode command to reserve a different VLAN as the internal usage VLAN of an interface. Use the `no` form of this command to restore the default configuration.

**Syntax**

- `ip internal-usage-vlan vlan-id`
- `no ip internal-usage-vlan`
**Parameters**

*vlan-id*—Specifies the internal usage VLAN ID.

**Default Configuration**

No VLAN is reserved as an internal usage VLAN by default (using this command).

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

**User Guidelines**

An internal usage VLAN is assigned by the system when an IP interface is defined on an Ethernet port or port-channel.

If an internal usage VLAN is not defined for a port, the software selects one of the unused VLANs.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do one of the following:

- Remove the IP address from the interface (this releases the internal usage VLAN).
- Recreate the VLAN on the required interface (now it will be assigned to the interface and not be used as an internal usage VLAN)
- Recreate the IP interface (another internal usage VLAN is assigned to this IP interface) or use this command to explicitly define the internal usage VLAN.

**Example**

The following example reserves unused VLAN 200 as the internal usage VLAN of gi3.

```
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# ip internal-usage-vlan 200
```

### 32.28 show vlan internal usage

Use the `show vlan internal usage` Privileged EXEC mode command to display a list of VLANs used internally by the device (defined by the user).
Syntax
show vlan internal usage

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays VLANs used internally by the device.

```
switchxxxxxx# show vlan internal usage

Usage       VLAN   Reserved   IP address
----------   ------   ---------   ---------
            1007     No        Active
            1008     Yes       Inactive
            1009     Yes       Active
```

32.29  switchport access multicast-tv vlan

Use the `switchport access multicast-tv vlan` Interface Configuration (Ethernet, Port-channel) mode command to enable receiving Multicast transmissions on an interface that is not the access port VLAN, while keeping the L2 segregation with subscribers on different access port VLANs. Use the `no` form of this command to disable receiving Multicast transmissions.

Syntax
```
switchport access multicast-tv vlan vlan-id
no switchport access multicast-tv vlan
```

Parameters

- `vlan-id`—Specifies the Multicast TV VLAN ID.
Default Configuration
Receiving Multicast transmissions is disabled.

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

User Guidelines
The user cannot transmit Multicast transmissions on the Multicast TV VLAN.
A Multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

Example
The following example enables gi5 to receive Multicast transmissions from VLAN 11.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11
```

32.30 switchport customer multicast-tv vlan
Use the `switchport customer multicast-tv vlan` Interface Configuration mode command to enable receiving Multicast transmissions from a VLAN that is not the customer port's VLAN, while keeping the L2 segregation with subscribers on different customer port VLANS.

Syntax
`switchport customer multicast-tv vlan [add vlan-list | remove vlan-list]`

Parameters
- `add vlan-list`—Specifies a list of Multicast TV VLANS to add to interface.
- `remove vlan-list`—Specifies a list of Multicast TV VLANS to remove from interface.

Default Configuration
The port is not a member in any Multicast TV VLAN.
**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

The user cannot transmit Multicast transmissions on Multicast TV VLANs.

A Multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

**Example**

The following example enables gi5 to receive Multicast transmissions from VLANs 5, 6, 7.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

**32.31 show vlan multicast-tv**

Use the `show vlan Multicast-tv` EXEC mode command to display the source and receiver ports of Multicast-TV VLAN. Source ports can transmit and receive traffic to/from the VLAN, while receiver ports can only receive traffic from the VLAN.

**Syntax**

```
show vlan Multicast-tv vlan vlan-id
```

**Parameters**

`vlan-id`—Specifies the VLAN ID.

**Default Configuration**

N/A

**Command Mode**

EXEC mode
Example

The following example displays information on the source and receiver ports of Multicast-TV VLAN 1000.

```
switchxxxxxx# show vlan multicast-tv vlan 1000
Source Ports  Receiver Ports
-------------  ---------------
  gi8, gi9     gi1-18
```

32.32  vlan prohibit-internal-usage

Use the `vlan prohibit-internal-usage` command in Global configuration mode to specify VLANs that cannot be used by the switch as internal VLANs.

Syntax

```
vlan prohibit-internal-usage [none | except] vlan-list
```

Parameters

- **none**—Remove all VLANs from User Reserved VLAN list.
- **except**—The User Reserved VLAN list includes all VLANs except the given ones.
- **vlan-list**—List of VLANs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. The VLAN IDs that can be used are from 1 through 4094.

Default Configuration

The User Reserved VLAN list is empty.

Command Mode

Global Configuration mode

User Guidelines

The switch requires an internal VLAN in the following cases:

- When an IP interface is defined directly on an Ethernet port or on a Port channel
• For each IPv6 tunnel, if IPv6 Routing is supported by the switch.

When a switch requires an internal VLAN, it takes a free VLAN with the highest VLAN_ID.

Use the **vlan prohibit-internal-usage** command to define a list of VLANs that cannot be selected as internal VLANs after reload.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do the following

- Add the VLAN to the prohibited User Reserved VLAN list.
- Copy the Running Configuration file to the Startup Configuration file
- Reload the switch
- Create the VLAN

**Example**

The following example specifies that VLANs 4010, 4012, and 4090-4094 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage except 4010,4012,4090-4094
```

### 32.33 show vlan internal usage

Use the **show vlan internal usage** Privileged EXEC mode command to display a list of VLANs used internally by the device (defined by the user).

**Syntax**

```
show vlan internal usage
```

**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC mode
### Example

The following example displays the VLANs that are used internally by the switch:

```
show vlan internal usage

User Reserved VLAN list after reset: 4080-4094
Current User Reserved VLAN list: 4090-4094

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>4094</td>
<td>gi12</td>
</tr>
<tr>
<td>4093</td>
<td>gi23</td>
</tr>
<tr>
<td>4092</td>
<td>tunnel 1</td>
</tr>
</tbody>
</table>
```
Voice VLAN Commands

33.1 voice vlan state

The `voice vlan state` Global Configuration mode command sets the type of voice VLAN that is functional on the device or disables voice VLAN entirely. The `no` format of the command returns to the default.

Syntax

```plaintext
voice vlan state {oui-enabled | auto-enabled | auto-triggered | disabled}
no voice vlan state
```

Parameters

- `oui-enabled`—Voice VLAN is of type OUI.
- `auto-enabled`—Auto Voice VLAN is enabled.
- `auto-triggered`—Auto Voice VLAN on the switch is in standby and is put into operation when the switch detects a CDP device advertising a voice VLAN or if a voice VLAN ID is configured manually on the switch.
- `disabled`—Voice VLAN is disabled.

Default Configuration

`auto-triggered`

Command Mode

Global Configuration mode

User Guidelines

By factory default, CDP, LLDP, and LLDP-MED are enabled on the switch. In addition, manual Smartport mode and Basic QoS with trusted DSCP is enabled. All ports are members of default VLAN 1, which is also the default Voice VLAN.

In addition, dynamic voice VLAN (`auto-triggered`) mode is the default mode of auto voice VLAN. In this mode, voice VLAN is enabled by a trigger (advertisement received by voice device attached to port).
If the administrative state is:

- **disabled** — The operational state is **disabled**.
- **oui-enabled** — The operational state is **oui-enabled**.
- **auto-enabled** — The operational state is **auto-enabled**.
- **auto-triggered** — The operational state is **auto-enabled** only if one of the following occurs:
  - A static local configured voice VLAN ID, CoS/802.1p, and/or DSCP that is not factory default is configured.
  - A CDP voice VLAN advertisement is received from a neighboring CDP device that is not a device of the same family as the current device.
  - A Voice Service Discovery Protocol (VSDP) message was received from a neighbor switch. VSDP is a Cisco Small Business proprietary protocol for SF and SG series managed switches.

In all other cases the operational state is **disabled**.

Notes:

- To change the administrative state from **oui-enabled** to **auto-enabled** (or **auto-triggered**), or vice versa, you must first set the administrative state to **disabled**.
- The administrative state cannot be set to **oui-enabled** if the Auto SmartPort administrative state is **enabled**.
- The administrative state cannot be set to **oui-enabled** if the voice VLAN is the default VLAN (VLAN 1) For **oui-enabled** mode, the voice VLAN cannot be 1.

Examples

**Example 1** - The following example enables the OUI mode of Voice VLAN. The first try did not work - it was necessary to first disable voice VLAN.

```
switchxxxxxx(config)# voice vlan state oui-enabled
```

Disable the voice VLAN before changing the voice VLAN trigger.

```
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# voice vlan state oui-enabled
```
Example 2 — The following example disables the Voice VLAN state. All auto Smartport configuration on ports are removed.

```
switchxxxxxx(config)#voice vlan state disabled
All interfaces with Auto Smartport dynamic type will be set to default.
Are you sure you want to continue? (Y/N) [Y] Y
```

```
switchxxxxxx(config)#30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 5
30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 8
30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 9
30-Apr-2011 00:04:41 %LINK-W-Down: Vlan 100
```

Example 3 — The following example sets the Voice VLAN state to auto-triggered. The VLANs are re-activated after auto SmartPort state is applied.

```
switchxxxxxx(config)#voice vlan state auto-triggered
```

```
switchxxxxxx(config)#30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 5
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 8
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 9
30-Apr-2011 00:13:52 %LINK-I-Up: Vlan 100
```

### 33.2 voice vlan refresh

The `voice vlan refresh` Global Configuration mode command restarts the Voice VLAN discovery process on all the Auto Voice VLAN-enabled switches in the VLAN by removing all externally learned voice VLAN attributes and resetting the voice VLAN to the default voice VLAN.

**Syntax**

- `voice vlan refresh`

**Parameters**

- N/A
Default Configuration

N/A

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# voice vlan refresh
switchxxxxxx(config)#

30-Apr-2011 02:01:02 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 100, VPT 5, DSCP 46 (Notification that Agreed Voice VLAN is updated)
(Auto Smartport configuration is changed)
30-Apr-2011 02:01:05 %LINK-W-Down: Vlan 50
30-Apr-2011 02:01:05 %LINK-W-Down: Vlan 100
30-Apr-2011 02:01:06 %LINK-I-Up: Vlan 50
30-Apr-2011 02:01:06 %LINK-I-Up: Vlan 100

switchxxxxxx#show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 100
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
(Following is the new active source)
Agreed Voice VLAN is received from switch b0:c6:9a:c1:da:00
Agreed Voice VLAN priority is 2 (active CDP device)
Agreed Voice VLAN-ID is 100
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Apr-30 02:01:02
```
33.3 voice vlan id

Use the voice vlan id Global Configuration mode command to statically configure the VLAN identifier of the voice VLAN. The no format of the command returns the voice VLAN to the default VLAN (1).

Syntax

voice vlan id vlan-id

no voice vlan id

Parameters

vlan id vlan-id—Specifies the voice VLAN (range 1-4094).

Default Configuration

VLAN ID 1.

Command Mode

Global Configuration mode

User Guidelines

If the Voice VLAN does not exist, it is created automatically. It will not be removed automatically by the no version of this command.

Example

The following example enables VLAN 35 as the voice VLAN on the device.

switchxxxxxx(config)# voice vlan id 35

For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as static voice VLAN which has higher priority than voice VLAN learnt from external sources.

Are you sure you want to continue? (Y/N)[Y] Y

30-Apr-2011 00:19:36 %VLAN-I-VoiceVlanCreated: Voice Vlan ID 104 was created.

switchxxxxxx(config)#30-Apr-2011 00:19:51 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 104, VPT 5, DSCP 46
33.4 voice vlan vpt

Use the `voice vlan vpt` Global Configuration mode command to specify a value of VPT (802.1p VLAN priority tag) that will be advertised by LLDP in the Network Policy TLV. The `no` format of the command returns the value to the default.

Syntax

```
voice vlan vpt vpt-value
no voice vlan vpt
```

Parameters

- `vpt vpt-value`—The VPT value to be advertised (range 0-7).

Default Configuration

```
5
```

Command Mode

Global Configuration mode

Example

The following example sets 7 as the voice VLAN VPT. A notification that the new settings are different than the old ones is displayed.

```
switchxxxxxx(config)# voice vlan vpt 7
```

For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as static voice VLAN which has higher priority than voice VLAN learnt from external sources.

Are you sure you want to continue? (Y/N)[Y]  Y

30-Apr-2011 00:24:52 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 5, DSCP 46

```
switchxxxxxx(config)#30-Apr-2011 00:25:07 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 104, VPT 7, DSCP 46
```
33.5 voice vlan dscp

Use the **voice vlan dscp** Global Configuration mode command to specify a value of DSCP that will be advertised by LLDP in the Network Policy TLV. The **no** format of the command returns the value to the default.

**Syntax**

```plaintext
voice vlan dscp dscp-value
no voice vlan dscp
```

**Parameters**

*dscp dscp-value*—The DSCP value (range 0-63).

**Default Configuration**

46

**Command Mode**

Global Configuration mode

**Example**

The following example sets 63 as the voice VLAN DSCP.

```
switchxxxxxx(config)# voice vlan dscp 63
```

For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as static voice VLAN which has higher priority than voice VLAN learnt from external sources.

Are you sure you want to continue? (Y/N) [Y] Y

30-Apr-2011 00:31:07 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 7, DSCP 46

switchxxxxxx(config)#30-Apr-2011 00:31:22 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID 104, VPT 7, DSCP 63
### 33.6 voice vlan oui-table

Use the `voice vlan oui-table` Global Configuration mode command to configure the voice OUI table. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
voice vlan oui-table {add mac-address-prefix | remove mac-address-prefix} [text]
```

```
no voice vlan oui-table
```

**Parameters**

- **add mac-address-prefix**—Adds the specified MAC address prefix to the voice VLAN OUI table (length: 3 bytes).
- **remove mac-address-prefix**—Removes the specified MAC prefix address from the voice VLAN OUI table (length: 3 bytes).
- **text**—Adds the specified text as a description of the specified MAC address to the voice VLAN OUI table (length: 1–32 characters).

**Default Configuration**

The default voice VLAN OUI table is:

<table>
<thead>
<tr>
<th>OUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:e0:bb</td>
<td>3COM Phone</td>
</tr>
<tr>
<td>00:03:6b</td>
<td>Cisco Phone</td>
</tr>
<tr>
<td>00:e0:75</td>
<td>Veritel Polycom Phone</td>
</tr>
<tr>
<td>00:d0:1e</td>
<td>Pingtel Phone</td>
</tr>
<tr>
<td>00:01:e3</td>
<td>Siemens AG Phone</td>
</tr>
<tr>
<td>00:60:b9</td>
<td>NEC/Philips Phone</td>
</tr>
<tr>
<td>00:0fe2</td>
<td>Huawei-3COM Phone</td>
</tr>
<tr>
<td>00:09:6e</td>
<td>Avaya Phone</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration mode
User Guidelines

The classification of a packet from VoIP equipment/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.

Since the number of IP phone manufacturers that dominates the market is limited and well known, the known OUI values are configured by default and OUIs can be added/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 description experimental
```

33.7 voice vlan cos mode

Use the `voice vlan cos mode` Interface Configuration mode command to select the OUI voice VLAN Class of Service (CoS) mode. Use the `no` form of this command to return to the default.

Syntax

```
voice vlan cos mode {src / all}
```

```
nov voice vlan cos mode
```

Parameters

- `src`—QoS attributes are applied to packets with OUIs in the source MAC address. See the User Guidelines of `voice vlan oui-table`.

- `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 voice packets.

```
switchxxxxxx(config)# voice vlan cos mode all
```

33.8 voice vlan cos

Use the `voice vlan cos` Global Configuration mode command to set the OUI Voice VLAN Class of Service (CoS). Use the `no` form of this command to restore the default configuration.

Syntax

```
voice vlan cos cos [remark]
no voice vlan cos
```

Parameters

- `cos cos`—Specifies the voice VLAN Class of Service value. (Range: 0–7)
- `remark`—Specifies that the L2 user priority is remarked with the CoS value.

Default Configuration

The default CoS value is 5.
The L2 user priority is not remarked by default.

Command Mode
Global Configuration mode

Example

The following example sets the OUI voice VLAN CoS to 7 and does not do remarking.

```
switchxxxxxx(config)# voice vlan cos 7
```
### 33.9 voice vlan aging-timeout

Use the `voice vlan aging-timeout` Global Configuration mode command to set the OUI Voice VLAN aging timeout interval. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
voice vlan aging-timeout minutes
no voice vlan aging-timeout
```

**Parameters**

- `aging-timeout minutes`—Specifies the voice VLAN aging timeout interval in minutes. (Range: 1–43200).

**Default Configuration**

1440 minutes

**Command Mode**

Global Configuration mode

**Example**

The following example sets the OUI Voice VLAN aging timeout interval to 12 hours.

```
switchxxxxxx(config)# voice vlan aging-timeout 720
```

### 33.10 voice vlan enable

Use the `voice vlan enable` Interface Configuration (Ethernet, Port-channel) mode command to enable OUI voice VLAN configuration on an interface. Use the `no` form of this command to disable OUI voice VLAN configuration on an interface.

**Syntax**

```
voice vlan enable
no voice vlan enable
```
Default Configuration
Disabled

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

User Guidelines
This command is applicable only if the voice VLAN state is globally configured as OUI voice VLAN (using voice vlan state).

The port is added to the voice VLAN if a packet with a source MAC address OUI address (defined by voice vlan oui-table) is trapped on the port. Note: The packet VLAN ID does not have to be the voice VLAN, it can be any VLAN.

The port joins the voice VLAN as a tagged port.

If the time since the last MAC address with a source MAC address OUI address was received on the interface exceeds the timeout limit (configured by voice vlan aging-timeout), the interface is removed from the voice VLAN.

Example
The following example enables OUI voice VLAN configuration on gi2.

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# voice vlan enable
```

33.11 show voice vlan
Use the show voice vlan EXEC mode command to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI.

Syntax
```
show voice vlan [type {oui|auto}] [interface-id | detailed]
```

Parameters
- **type oui**—Common and OUI-voice-VLAN specific parameters are displayed.
- **type auto**—Common and Auto Voice VLAN-specific parameters are displayed.
Voice VLAN Commands

- **interface-id**— Specifies an Ethernet port ID. Relevant only for the OUI type.
- **detailed**— Displays information for non-present ports in addition to present ports. Only valid when type is oui.

**Default Configuration**

If the **type** parameter is omitted the current Voice VLAN type is used.

If the **interface-id** parameter is omitted then information about all interfaces is displayed.

All ports are displayed. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC mode

**User Guidelines**

Using this command without parameters displays the current voice VLAN type parameters and local and agreed voice VLAN settings.

Using this command with the **type** parameter displays the voice VLAN parameters relevant to the type selected. The the local and agreed voice VLAN settings are displayed only if this is the current voice VLAN state.

The **interface-id** parameter is relevant only for the OUI VLAN type.

**Examples**

The following examples display the output of this command in various configurations.

**Example 1** - Displays the **auto** voice VLAN parameters (this is independent of the voice VLAN state actually enabled).

```
switch>show voice vlan type auto
switchxxxxxx#show voice vlan type auto
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
```
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
switchxxxxxx#

**Example 2**—Displays the current voice VLAN parameters when the voice VLAN state is auto-enabled.

```
switch>show voice vlan
Administrate Voice VLAN state is auto-enabled
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is 0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 16:48:13
switchxxxxxx#
```

**Example 3**—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered but voice VLAN has not been triggered.

```
switch>show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is disabled
VSDP Authentication is disabled
```

**Example 4**—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered and it has been triggered.

```
switchxxxxxx(config)#voice vlan state auto-triggered
switchxxxxxx(config)#voice vlan state auto-triggered
```
operational voice vlan state is auto
admin state is auto triggered
switchxxxxxx#show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is 0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51

Example 5—Displays the current voice VLAN parameters when both auto voice VLAN and OUI are disabled.

switch>show voice vlan
switchxxxxxx#show voice vlan
Administrate Voice VLAN state is disabled
Operational Voice VLAN state is disabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Aging timeout: 1440 minutes

Example 5—Displays the voice VLAN parameters when the voice VLAN operational state is OUI.

switch>show voice vlan
Administrate Voice VLAN state is oui-enabled
Operational Voice VLAN state is oui-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 4
Best Local DSCP is 1
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes
OUI table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:E0:BB</td>
<td>3COM</td>
</tr>
<tr>
<td>00:03:6B</td>
<td>Cisco</td>
</tr>
<tr>
<td>00:E0:75</td>
<td>Veritel</td>
</tr>
<tr>
<td>00:D0:1E</td>
<td>Pingtel</td>
</tr>
<tr>
<td>00:01:E3</td>
<td>Simens</td>
</tr>
<tr>
<td>00:60:B9</td>
<td>NEC/Philips</td>
</tr>
<tr>
<td>00:0F:E2</td>
<td>Huawei-3COM</td>
</tr>
<tr>
<td>00:09:6E</td>
<td>Avaya</td>
</tr>
</tbody>
</table>

Interface | Enabled | Secure | Activated | CoS Mode |
-----------|---------|--------|-----------|----------|
            | ------- | ------ |-----------|----------|
gi1         | Yes     | Yes    | Yes       | all      |
gi2         | Yes     | Yes    | No        | src      |
gi3         | No      | No     |            |          |
...         |         |        |           |          |

### 33.12 show voice vlan local

The `show voice vlan local` EXEC mode command displays information about the auto voice VLAN local configuration, including the best local voice VLAN.

**Syntax**

`show voice vlan local`
Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Examples

Example 1 - A CDP device is connected to an interface and a conflict is detected:

30-Apr-2011 00:39:24 %VLAN-W-ConflictingCDPDetected: conflict detected between operational VLAN and new CDP device 00:1e:13:73:3d:62 on interface gi7. Platform TLV is -4FXO-K9, Voice VLAN-ID is 100...

switchxxxxxx#show voice vlan local

Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
VSDP Authentication is enabled, key string name is alpha
The character '*' marks the best local Voice VLAN

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>VPT</th>
<th>DSCP</th>
<th>Source</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>46</td>
<td>default</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>*104</td>
<td>7</td>
<td>63</td>
<td>static</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>100</td>
<td></td>
<td></td>
<td>CDP</td>
<td>00:1e:13:73:3d:62</td>
<td>gi7</td>
</tr>
</tbody>
</table>

Example 2—Displays the local voice VLAN configuration when the voice VLAN state is auto-triggered.

switchxxxxxx#show voice vlan local

Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>VPT</th>
<th>DSCP</th>
<th>Source</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>46</td>
<td>default</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
Example 3—Displays the local voice VLAN configuration when the voice VLAN state is OUI.

```
switchxxxxxx#show voice vlan local

Administrative Voice VLAN state is auto-OUI
Operational Voice VLAN state is OUI

The character '*' marks the best local Voice VLAN

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>VPT</th>
<th>DSCP</th>
<th>Source</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>default</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>*10</td>
<td>1</td>
<td>27</td>
<td>static</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>10</td>
<td>CDP</td>
<td></td>
<td>00:00:12:ea:87:dc</td>
<td>gi1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>CDP</td>
<td></td>
<td>00:00:aa:aa:89:dc</td>
<td>po1</td>
<td></td>
</tr>
</tbody>
</table>
```

The character "*" marks the best local voice VLAN.
SSD Commands

34.1 ssd config

Use `ssd config` in Global Configuration to enter the Secure Sensitive Data (SSD) command mode. In this command mode, an administrator can configure how the sensitive data on the device, such as keys and passwords, is to be protected.

Syntax

```
ssd config
```

Command Mode

Global Configuration mode

User Guidelines

Only users with sufficient permission can use this command, which edits and displays the SSD configuration. See `ssd rule` for a description of these permissions.

Example

```
switchxxxxxx(config)# ssd config
switchxxxxxx(ssd-config)#
```

34.2 passphrase

Use `passphrase` in SSD Command mode to change the passphrase in the system. A device protects its sensitive data by encrypting them using the key generated from the passphrase.

Use the `no passphrase` to reset the passphrase to the default passphrase.

Syntax

```
passphrase [passphrase]
encrypted passphrase [encrypted-passphrase]
no passphrase
```
Parameters

- **passphrase** - New system passphrase.
- **encrypted-passphrase** - The passphrase in its encrypted form.

Default Usage

If this command is not entered, the default passphrase is used.

Command Mode

SSD Command Mode

User Guidelines

To use this command, enter passphrase and Enter, a confirmation message is displayed and the user must confirm the intention to change the passphrase. Then the passphrase can be entered (see example).

Encrypted passphrase is allowed only in the SSD Control Block of a source file that is being copied to the startup configuration file (user cannot manually enter this command).

When generating a passphrase, the user must use 4 different character classes (similar to strong password/passwords complexity). These can be: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.

Example

The following example defines a decrypted passphrase.

switchxxxxxx(ssd-config)# passphrase
This operation will change the system SSD passphrase. Are you sure? (Y/N) [N] Y
Please enter SSD passphrase:**********
Please reenter SSD passphrase:**********

34.3 ssd rule

Use `ssd rule` in SSD Command mode to configure an SSD rule. A device grants read permission of sensitive data to user based on the SSD rules. A user that is granted Both or Plaintext read permission is also granted permission to enter SSD Command Mode.

Use `no ssd rule` to delete user-defined rules and restore default rules.
Syntax

[encrypted] SSD rule {all | level-15 | default-user | user user-name} {secure | insecure | secure-xml-snmp | insecure-xml-snmp}
permission {encrypted-only | plaintext-only | both | exclude}
default-read {encrypted | plaintext | exclude}

no ssd rule [ {all | level-15 | default-user | user user-name} {secure | insecure | secure-xml-snmp | insecure-xml-snmp}]

Command Mode
SSD command mode.

Default Rules
The device has the following factory default rules:

Table 4: Default SSD Rules

<table>
<thead>
<tr>
<th>Rule Key</th>
<th>Channel</th>
<th>Read Permission</th>
<th>Default Read Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-15</td>
<td>secure-xml-snmp</td>
<td>Plaintext Only</td>
<td>Plaintext</td>
</tr>
<tr>
<td>level-15</td>
<td>secure</td>
<td>Both</td>
<td>Encrypted</td>
</tr>
<tr>
<td>level-15</td>
<td>insecure</td>
<td>Both</td>
<td>Encrypted</td>
</tr>
<tr>
<td>all</td>
<td>insecure-xml-snmp</td>
<td>Exclude</td>
<td>Exclude</td>
</tr>
<tr>
<td>all</td>
<td>secure</td>
<td>Encrypted Only</td>
<td>Encrypted</td>
</tr>
<tr>
<td>all</td>
<td>insecure</td>
<td>Encrypted Only</td>
<td>Encrypted</td>
</tr>
</tbody>
</table>

User Guidelines

Use **no ssd rule** to delete a user-defined rule or to restore the default of a modified default rule.

Use **no ssd rule** (without parameters) to remove all SSD rules and restore the default SSD rules. A confirmation message will be displayed asking permission to do this.

To delete specific rules (applicable for the user defined), provide parameters specifying the user and security of the channel.

**encrypted SSD rule** is used to copy an SSD rule from one device to another in a secure manner.
You can modify but cannot delete the default SSD rules. The following is the order in which SSD rules are applied:

- The SSD rules for specified *users*.
- The SSD rule for the default-user *(cisco)*.
- The SSD rules for level-15 users.
- The remaining SSD rules for all.

The user can enter the commands in any order. The ordering is done implicitly by the device.

**Examples**

**Example 1** - The following example modifies a rule.

```bash
switchxxxxxx(ssd-config)#ssd rule level-15 secure permission encrypted-only default-read encrypted
```

**Example 2** - The following example adds a rule.

```bash
switchxxxxxx(ssd-config)#ssd rule user james secure permission both default-read encrypted
```

**Example 3** - The following example adds a rule as encrypted format.

```bash
switchxxxxxx(ssd-config)#encrypted ssd rule iurwe874jho32iu9ufjo32i83232fdefsd
```

**Example 4** - The following example deletes a default rule.

```bash
switchxxxxxx(ssd-config)#no ssd rule all secure
```

**Example 5** - The following example deletes a user-defined rule.

```bash
switchxxxxxx(ssd-config)#no ssd rule user james secure
```

**Example 6** - The following example deletes all rules.

```bash
switchxxxxxx(ssd-config)#no ssd rule
```

This operation will delete all user-defined rules and retrieve the default rules instead.

Are you sure (Y/N): N
34.4 show SSD

Use `show ssd rules` in SSD Command mode to present the current SSD rules; the rules will be displayed as plaintext.

**Syntax**

```
show SSD [rules | brief]
```

**Parameters**

- `rules` - Display only the SSD rules.
- `brief` - Display the encrypted passphrase, File Passphrase Control and File Integrity attributes.

**Command Mode**

SSD Command mode

Privileged EXEC mode

**Default Configuration**

Display all SDD information.

**Examples**

**Example 1** - The following example displays all SSD information.

```
switchxxxxxx(ssd-config)#show ssd
```

SSD current parameters:
- Local Passphrase: Default
- File Passphrase Control: Unrestricted
- File Integrity Control: Disabled

SSD parameters after reset:
- Local Passphrase: Default
- File Passphrase Control: Unrestricted
- File Integrity Control: Disabled

<table>
<thead>
<tr>
<th>User Type</th>
<th>User Name</th>
<th>Channel</th>
<th>Read Permission</th>
<th>Default Read</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific</td>
<td>admin11</td>
<td>secure</td>
<td>Both</td>
<td>Encrypted</td>
<td>User-Define</td>
</tr>
<tr>
<td>Specific</td>
<td>admin2</td>
<td>secure</td>
<td>Encrypted-Only</td>
<td>Encrypted</td>
<td>User-Define</td>
</tr>
<tr>
<td>Level-15</td>
<td></td>
<td>secure-xml-snmp</td>
<td>Plaintext-Only</td>
<td>Plaintext</td>
<td>Default</td>
</tr>
</tbody>
</table>
Example 2 - The following example displays the SSD rules.

```
switchxxxxxx(ssd-config)# show ssd rules

User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
Specific    admin11       secure            Both        Encrypted   User-Define
Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
Level-15                  secure            Both        Encrypted     Default
Level-15                 insecure           Both        Encrypted     Default
All                     secure       Encrypted-Only   Encrypted     Default
All                    insecure      Encrypted-Only   Encrypted     Default
All                insecure-xml-snmp Plaintext-Only   Plaintext    *Default

* Modified default entry
```

Example 3 - The following example displays the SSD attributes.

```
switchxxxxxx(ssd-config)# show ssd brief

SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled

SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
```

34.5   ssd session read

Use **ssd session read** in Global Configuration mode to override the current SSD default read of the current session.
Syntax

ssd session read {encrypted | plaintext | exclude}

no ssd session read

Parameters

- **encrypted** - Override the SSD default option to encrypted
- **plaintext** - Override the SSD default option to plaintext
- **exclude** - Override the SSD default option to exclude

Command Mode

Global configuration mode.

Default

The command itself does not have a default. However, note that the read mode of the session itself, defaults to the default read mode of the SSD rule that the device uses to grant SSD permission to the user of the session.

User Guidelines

Use no ssd session read to restore the default read option of the SSD rules. This configuration will be allowed only if the user of the current session has sufficient read permissions; otherwise, the command will fail and an error will be displayed. The setting will take effect immediately and will terminate when the user restores the settings or exits the session.

Example

```
switchxxxxxx(config)# ssd session read plaintext
```

### 34.6 show ssd session

Use **show ssd session** in Exec mode to view the SSD read permission and default read mode of the user of the current session.

Syntax

show ssd session
**Command Mode**

EXEC mode.

**Default**

N/A

**Examples**

switchxxxxx# show ssd session

User Name/Level: James / Level 15

User Read Permission: Both

Current Session Read mode: Plaintext

---

### 34.7 ssd file passphrase control

Use `ssd file passphrase control` in SSD Command mode to provide an additional level of protection when copying configuration files to the startup configuration file. The passphrase in a configuration file is always encrypted with the default passphrase key.

**Syntax**

`ssd file passphrase control {restricted | unrestricted}`

`no ssd file passphrase control`

**Parameters**

- **Restricted** - In this mode, a device restricts its passphrase from being exported into a configuration file. Restricted mode protects the encrypted sensitive data in a configuration file from devices that do not have the passphrase. The mode should be used when a user does not want to expose the passphrase in a configuration file.

- **Unrestricted** - In this mode, a device will include its passphrase when creating a configuration file. This allows any devices accepting the configuration file to learn the passphrase from the file.

**Default**

The default is `unrestricted`. 
**Command Mode**

SSD Command mode.

**User Guidelines**

To revert to the default state, use the no ssd file passphrase control command.

Note that after a device is reset to the factory default, its local passphrase is set to the default passphrase. As a result, the device will not be able to decrypted sensitive data encrypted with a user-defined passphrase key in its own configuration files until the device is manually configured with the user-passphrase again or the files are created in unrestricted mode.

If a user-defined passphrase in Unrestricted mode is configured, it is highly recommended to enable SSD File Integrity Control. Enabling SSD File Integrity Control protects configuration files from tampering.

Any modification made to a configuration file that is integrity-protected is considered to be tampering.

**Examples**

```
console(ssd-config)# ssd file passphrase control restricted
console(ssd-config)# no ssd file passphrase control
```

### 34.8 ssd file integrity control

Use ssd file integrity control command in SSD Command Mode to instruct the device to protect newly-generated configuration files that contain encrypted sensitive data from tampering.

Use no ssd file integrity control to disable Integrity Control.

**Syntax**

```
ssd file integrity control enabled
no ssd file integrity control
```

**Parameters**

- **enabled** - Enable file integrity control to protect newly-generated configuration files from tampering.
Default
The default file input control is disable.

Command Mode
SSD Command Mode.

User Guidelines
TA user can protect a configuration file from being tampered by creating the file with File Integrity Control enabled. It is recommended that File Integrity Control be enabled when a devices users a user-defined passphrase with Unrestricted Configuration File Passphrase Control.

A device determines whether the integrity of a configuration file is protected by examining the File Integrity Control command in the file. If a file in integrity-protected, but a device finds the integrity of the file is not intact, the device rejects the file. Otherwise, the file is accepted for further processing.

Examples
switchxxxxxx(ssd-config)# ssd file integrity control enabled

When File Integrity is enabled, an internal digest command is added to the end of the entire configuration file. This is used in downloading the configuration file to the startup configuration.

config-file-digest 0AC78001122334400AC780011223344
35.1 macro auto (Global)

The macro auto Global Configuration mode command sets the Auto Smartports administrative global state. The no format of the command returns to the default.

Syntax

macro auto {enabled | disabled | controlled}

no macro auto

Parameters

- **enabled**—Auto Smartport administrative global and operational states are enabled.
- **disabled**—Auto Smartport administrative global and operational states are disabled.
- **controlled**—Auto Smartport administrative global and operational states are enabled when Auto Voice VLAN is in operation.

Default Configuration

Administrative state is **controlled**.

Command Mode

Global Configuration mode

User Guidelines

Regardless of the status of Auto Smartport, you can always manually apply a Smartport macro to its associated Smartport type. A Smartport macro is either a built-in macro or a user-defined macro. You can define and apply a macro using the CLI commands presented in the Macro Commands section.

If the Auto Smartport Administrative state is controlled, the Auto Smartport Operational state is managed by the Voice VLAN manager and is set as follows:

- Auto Smartport Operational state is disabled when the OUI Voice VLAN is enabled.
- Auto Smartport Operational state is enabled when the Auto Voice VLAN is enabled.

A user cannot enable Auto Smartport globally if the OUI Voice VLAN is enabled.

**Example**

This example shows an attempt to enable the Auto Smartport feature globally in the controlled mode. This is not possible because the OUI voice feature is enabled. The voice VLAN state is then disabled, after which Auto Smartports can be enabled. The appropriate VLANs are automatically enabled because the ports are configured for Auto Smartports on these VLANs.

```
switchxxxxxx(config)# macro auto controlled
switchxxxxxx(config)# macro auto enabled
Auto smartports cannot be enabled because OUI voice is enabled.
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# macro auto enabled
switchxxxxxx(config)# 10-Apr-2011 16:11:31 %LINK-I-Up: Vlan 20
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 5
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 6
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 7
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 8
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 9
10-Apr-2011 16:11:33 %LINK-I-Up: Vlan 10
```

### 35.2 macro auto smartport (Interface)

The **macro auto smartport** Interface Configuration mode command enables the Auto Smartport feature on a given interface. The **no** format of the command disables the feature on the interface.

**Syntax**

```
macro auto smartport
no macro auto smartport
```
Parameters
N/A

Default Configuration
Enabled.

Command Mode
Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines
This command is effective only when Auto Smartport is globally enabled.

Example
Enables the Auto Smartport feature on port 1:

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)# macro auto smartport
```

35.3 macro auto trunk refresh

The `macro auto trunk refresh` Global Configuration command reapplyes the Smartport macro on a specific interface, or to all the interfaces with the specified Smartport type.

Syntax

```
macro auto trunk refresh [smartport-type] [interface-id]
```

Parameters

- `smartport-type`—Smartport type (switch, router, wireless access point (ap))
- `interface-id`—Interface Identifier (port or port channel).

Default Configuration
See User Guidelines.
**Command Mode**

Global Configuration mode

**User Guidelines**

The `macro auto smartport` command becomes effective only when the Auto Smartport is globally enabled.

If both `smartport-type` and `interface-id` are defined, the attached Smartport macro is executed on the interface if it has the given Smartport type.

If only `smartport-type` is defined, the attached Smartport macro is executed on all interfaces having the given Smartport type.

If only `interface-id` is defined then the corresponding attached Smartport macro is executed if the interface has one of the following Smartport types: `switch`, `router` or wireless access point (ap).

If a Smartport macro contains configuration commands that are no longer current on one or more interfaces, you can update their configuration by reapplying the Smartport macro on the interfaces.

**Example**

Adds the ports of Smartport type `switch` to all existing VLANs by running the associated Smartport macros.

```plaintext
switchxxxxxx(config)# macro auto trunk refresh switch
```

### 35.4 `macro auto resume`

The `macro auto resume` Interface Configuration mode command changes the Smartport type from `unknown` to `default` and resumes the Smartport feature on a given interface (but does not reapply the Smartport macro; this is done by `macro auto trunk refresh`).

**Syntax**

`macro auto resume`

**Parameters**

N/A
Default Configuration
N/A

Command Mode
Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines
When a Smartport macro fails at an interface, the Smartport type of the interface becomes Unknown. You must diagnose the reason for the failure on the interface and/or Smartport macro, and correct the error. Before you or Auto Smartport are allowed to reapply the desired Smartport macro, you must reset the interface using the `macro auto resume` command, which changes the Smartport type of the interface to Default. Then you can run `macro auto trunk refresh`.

Example
Changes the Smartport type from unknown to default and resumes the Smartport feature on port 1.

```
switchxxxxx(config) interface gi1
switchxxxxx(config-if)#macro auto resume
```

35.5 macro auto persistent

The `macro auto persistent` Interface Configuration mode command sets the interface as a Smartport persistent interface. The `no` format of the command returns it to default.

Syntax
- `macro auto persistent`
- `no macro auto persistent`

Parameters
- N/A

Default Configuration
Not persistent.
Command Mode

Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines

A Smartport’s persistent interface retains its dynamic configuration in the following cases: link down/up, the attaching device ages out, and reboot. Note that for persistence and the Smartport configuration to be effective across reboot, the Running Configuration file must be saved to the Startup Configuration file.

Example

The example establishes two port ranges and makes one persistent and the other not.

```
switchxxxxxx(config)#interface range gi1-2
switchxxxxxx(config-if-range)#macro auto persistent
switchxxxxxx(config-if-range)#exit
switchxxxxxx(config)#interface range gi3-4
switchxxxxxx(config-if-range)#no macro auto persistent
```

35.6 macro auto smartport type

The `macro auto smartport type` Interface Configuration mode command manually (statically) assigns a Smartport type to an interface. The `no` format of the command removes the manually-configured type and returns it to default.

Syntax

```
macro auto smartport type smartport-type [parameter-name value
[parameter-name value [parameter-name value]]
```

Parameters

- `smartport type smartport-type`—Smartport type.
- `parameter-name value`—Specifies the parameter name and its value (Range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).
Default Configuration

`parameter-name value`—Parameter default value. For instance, if the parameter is the voice VLAN, the default value is the default voice VLAN.

Command Mode

Interface Configuration mode (Ethernet Interface, Port Channel)

User Guidelines

A static type set by the command cannot be changed by a dynamic type.

Example

This example shows an attempt to set the Smartport type of port 1 to printer (statically). The macro fails at line 10. The `show parser macro name` command is run to display the contents of the macro printer in order to see which line failed.

```
switchxxxxxx(config) interface gi1
switchxxxxxx(config-if)#macro auto smartport type printer
30-May-2011 15:02:45 %AUTOSMARTPORT-E-FAILED_MACRO: Macro printer for auto smartport type Printer on interface gi1 failed at command number 10
switchxxxxxx(config-if)#exit
switchxxxxxx(config-if)#do show parser macro name printer
Macro name : printer
Macro type : default interface
1. #macro description printer
2. #macro keywords $native_vlan
3. #
4. #macro key description: $native_vlan: The untag VLAN which will be configured on the port
5. #Default Values are
6. #$native_vlan = Default VLAN
7. #
8. #the port type cannot be detected automatically
9. #
```
10. switchport mode access
11. switchport access vlan $native_vlan
12. #
13. #single host
14. port security max 1
15. port security mode max-addresses
16. port security discard trap 60
17. #
18. smartport storm-control broadcast level 10
19. smartport storm-control include-multicast
20. smartport storm-control broadcast enable
switch030008(config)#

35.7  macro auto processing cdp

The **macro auto processing cdp** Global Configuration mode command enables using CDP capability information to identify the type of an attached device.

When Auto Smartport is enabled on an interface and this command is run, the switch automatically applies the corresponding Smartport type to the interface based on the CDP capabilities advertised by the attaching device(s).

The no format of the command disables the feature.

**Syntax**

macro auto processing cdp

no macro auto processing cdp

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Global Configuration
Example
To enable CDP globally:

```
switchxxxxxx(config)#macro auto processing cdp
```

### 35.8  macro auto processing lldp

The `macro auto processing lldp` Global Configuration mode command enables using the LLDP capability information to identify the type of an attached device.

When Auto Smartport is enabled on an interface and this command is run, the switch automatically applies the corresponding Smartport type to the interface based on the LLDP capabilities advertised by the attaching device(s).

The `no` format of the command disables the feature.

**Syntax**

```
macro auto processing lldp
no macro auto processing lldp
```

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Global Configuration

**Example**

To enable LLDP globally:

```
switchxxxxxx(config)#macro auto processing lldp
```
35.9 macro auto processing type

The **macro auto processing type** Global Configuration mode command enables or disables automatic detection of devices of given type. The no format of the command returns to the default.

**Syntax**

```
macro auto processing type smartport-type {enabled | disabled}
no macro auto processing type smartport-type
```

**Parameters**

smartport-type—Smartport type (range: host, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

**Default Configuration**

By default, auto detection of ip_phone, ip_phone_desktop, switch, and wireless access point (ap) is enabled.

**Command Mode**

Global Configuration

**Example**

In this example, automatic detection of wireless access points (ap) is enabled.

```
switchxxxxxx(config)# macro auto processing type ?
host set type to host
ip_phone set type to ip_phone
ip_phone_desktop set type to ip_phone_desktop
switch set type to switch
router set type to router
ap set type to access point
switchxxxxxx(config)# macro auto processing type ap enabled
```
### 35.10 macro auto user smartport macro

The **macro auto user smartport macro** Global Configuration mode command links user-defined Smartport macros to a Smartport type. This is done by replacing the link to the built-in macro with the link to the user-defined macro. The **no** format of the command returns the link to the default built-in Smartport macro.

**Syntax**

```
macro auto user smartport macro smartport-type user-defined-macro-name
[parameter-name value [parameter-name value [parameter-name value]]]
```

```
no macro auto user smartport macro smartport-type
```

**Parameters**

- **smartport macro smartport-type**—Smartport type (range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

- **smartport macro user-defined-macro-name**—Specifies the user-defined macro name that replaces the built-in Smartport macro.

- **parameter-name value**—Specifies the parameter name and its value in the user-defined macro.

**Default Configuration**

**parameter-name value**—Parameter’s default value. For instance, if the parameter is the native VLAN, the default value is the default native VLAN.

**Command Mode**

Global Configuration

**User Guidelines**

The scope of each parameter is the macro in which it is defined, with the exception of the parameter `$voice_vlan`, which is a global parameter and its value is specified by the switch and cannot be defined in a macro.

The macros must be defined before linking them in this command.

Smartport macros must be disconnected from the Smartport type before removing them (using the **no** version of this command).

To associate a Smartport type with a user-defined macros, you must have defined a pair of macros: one to apply the configuration, and the other (anti macro) to
remove the configuration. The macros are paired by their name. The name of the anti macro is the concatenation of no_ with the name of the corresponding macro. Please refer to the Macro Command section for details about defining macro.

Example
To link the user-defined macro: my_ip_phone_desktop to the Smartport type: ip_phone_desktop and provide values for its two parameters:

```
switchxxxxxx(config)\# macro auto user smartport macro ip_phone_desktop my_ip_phone_desktop $p1 1 $p2 2
```

### 35.11 macro auto built-in parameters

The macro auto built-in parameters Global Configuration mode command replaces the default Auto Smartport values of built-in Smartport macros. The no format of the command returns to the default values.

**Syntax**

```
macro auto built-in parameters smartport-type [parameter-name value [parameter-name value [parameter-name value]]]
```

```
no macro auto built-in parameters smartport-type
```

**Parameters**

- **smartport-type**—Smartport type (range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

- **parameter-name value**—Specifies the parameter name and its value. These are the parameters of the built-in or user-defined macro defined in macro auto user smartport macro.

**Default Configuration**

The default value of parameter $native_vlan of the built-in Smartport macros is 1.

For other parameters, the default value is the parameter’s default value. For instance, if the parameter is the native VLAN, the default value is the default native VLAN.
Command Mode

Global Configuration

User Guidelines

By default, each Smartport type is associated with a pair of built-in macros: a macro that applies the configuration and the anti macro (no macro) to remove the configuration. The Smartport types are the same as the name of the corresponding built-in Smartport macros, with the anti macro prefixed with no_. The value of the parameter $voice_vlan cannot be changed by this command.

Example

To change the parameters of a built-in macro:

```
switchxxxxxx(config) macro auto built-in parameters switch $native_vlan 2
```

35.12 show macro auto processing

The show macro auto processing EXEC mode command displays information about which protocols (CDP/LLDP) are enabled and which device types can be detected automatically.

Syntax

show macro auto processing

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC

Example

```
switchxxxxxx#show macro auto processing
```
CDB: enabled
LLDP: enabled
host: disabled
ip_phone: enabled
ip_phone_desktop: enabled
switch: enabled
router: disabled
ap: enabled

35.13 show macro auto smart-macros

The show macro auto smart-macros EXEC mode command displays the name of Smartport macros, their type (built-in or user-defined) and their parameters. This information is displayed for all Smartport types or for the specified one.

Syntax

show macro auto smart-macros [smartport-type]

Parameters

smartport-type—Smartport type (range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

Default Configuration

N/A

Command Mode

EXEC

Example

switchxxxxxx#show macro auto smart-macros
SG300-52-R#show macro auto smart-macros
SmartPort type : printer
Parameters : $native_vlan=1
SmartPort Macro: printer (Built-In)
SmartPort type : desktop
Parameters : $max_hosts=10 $native_vlan=1
SmartPort Macro: desktop (Built-In)

SmartPort type : guest
Parameters : $native_vlan=1
SmartPort Macro: guest (Built-In)

SmartPort type : server
Parameters : $max_hosts=10 $native_vlan=1
SmartPort Macro: server (Built-In)

SmartPort type : host
Parameters : $max_hosts=10 $native_vlan=1
SmartPort Macro: host (Built-In)

SmartPort type : ip-camera
Parameters : $native_vlan=1
SmartPort Macro: ip_camera (Built-In)

SmartPort type : ip-phone
Parameters : $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone (Built-In)

SmartPort type : ip-phone-desktop
Parameters : $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone_desktop (Built-In)

SmartPort type : switch
Parameters : $native_vlan=1 $voice_vlan=1
SmartPort Macro: switch (Built-In)

SmartPort type : router
Parameters : $native_vlan=1 $voice_vlan=1
SmartPort Macro: router (Built-In)

SmartPort type : ap
Parameters : $native_vlan=1 $voice_vlan=1
SmartPort Macro: ap (Built-In)

SG300-52-R#
35.14  show macro auto ports

The `show macro auto ports` EXEC mode command displays information about all Smartport ports or a specific one. If a macro was run on the port and it failed, the type of the port is displayed as Unknown.

**Syntax**

`show macro auto ports [interface-id | detailed]`

**Parameters**

- **interface-id**—Interface Identifier (Ethernet interface, port channel)
- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display information for all interfaces. If detailed is not used, only present ports are displayed.

**Command Mode**

EXEC

**Examples**

**Example 1** - Note that Smartport on switch and phone types was configured automatically. Smartport on routers was configured statically.

```
switchxxxxxx# show macro auto ports
Smartport is enabled
Administrative Globally Auto Smartport is enabled
Operational Globally Auto Smartport is enabled
Interface    Auto Smartport  Persistent  Smartport Type
             Admin State     State
-----------------  ----------- ---------------
  gi1          disabled        enabled     switch
  gi2          enabled         enabled     default
  gi3          enabled         disabled    phone
  gi4          enabled         enabled     router (static)
```
Example 2 - Disabling auto SmartPort on gi2:

```
switchxxxxxx(config-if)#interface gi2
switchxxxxxx(config-if)#no macro auto smartport
switchxxxxxx(config-if)#end

switchxxxxxx#show macro auto ports gi2
SmartPort is Enabled
Administrative Globally Auto SmartPort is controlled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is disabled on gi2
Persistent state is not-persistent
Interface type is default
No macro has been activated
```

Example 3—Enabling auto Smartport on gi1:

```
switchxxxxxx(config-if)#interface gi1
switchxxxxxx(config-if)#macro auto smartport
switchxxxxxx(config-if)#end

switchxxxxxx#show macro auto ports gi1
SmartPort is Enabled
Administrative Globally Auto SmartPort is enabled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is enabled on gi1
Persistent state is persistent
Interface type is switch
Last activated macro is switch
```
35.15 smartport switchport trunk allowed vlan

The smartport switchport trunk allowed vlan Interface Configuration (Ethernet, port-channel) mode command adds/removes VLANs to/from a trunk port.

Syntax

smartport switchport trunk allowed vlan {add [vlan-list / all] | remove [vlan-list / all]}

Parameters

- **add vlan-list**—Specifies a list of VLAN IDs to add to interface. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **add all**—Add all VLANs to interface.
- **remove vlan-list**—Specifies a list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **remove all**—Remove all VLANs from interface.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command is an extension of the switchport trunk allowed vlan command. Unlike the switchport trunk allowed vlan command, the vlan-list parameter of this command may include the voice VLAN (when it is the default VLAN). If the default VLAN is the voice VLAN, the following occurs:

- **add all** — Adds the interface to the default VLAN as an egress tagged port.
- **remove all** — Removes the interface from the default VLAN.

Example

To add port 1 to VLANs 1-5:

```
switchxxxxxx(config)#interface gi1
```
35.16  smartport switchport trunk native vlan

Use the `smartport switchport trunk native vlan` Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN when the interface is in trunk mode. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
smartport switchport trunk native vlan native-vlan-id
```

**Parameters**

`native-vlan-id`—Specifies the native VLAN ID.

**Default Configuration**

VLAN 1

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

This command is an extension of the `switchport trunk native vlan` CLI command. Unlike the `switchport trunk native vlan` CLI command, this command may also be applied to the default VLAN when the interface belongs to the default VLAN as egress tagged port.

**Example**

Define the native VLAN when port 1 is in trunk mode:

```
switchxxxxxx(config-if)# smartport switchport trunk allowed vlan add 1-5
```

---

35.17  smartport storm-control broadcast enable

Use the `smartport storm-control broadcast enable` Interface Configuration (Ethernet, port-channel) mode command to enable storm control on a Smartport port. Use the `no` form of this command to disable storm control.
### Syntax

`smartport storm-control broadcast enable`

#### Parameters

N/A

#### Default Configuration

N/A

#### Command Mode

Interface Configuration (Ethernet, port-channel) mode

#### Example

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)#smartport storm-control broadcast enable
```

### 35.18  `smartport storm-control broadcast level`

Use the `smartport storm-control broadcast level` Interface Configuration (Ethernet, port-channel) mode command to control the amount of Broadcast traffic allowed on an interface.

#### Syntax

`smartport storm-control broadcast level {level | kbps kbps}
no smartport storm-control broadcast level`

#### Parameters

- **level**—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1 -100)
- **kbps**—Maximum of kilobits per second of broadcast traffic on a port. (Range 70–10000000)

#### Default Configuration

- **level**—10%
- **kbps**—10% of port speed in Kbps
Smartport Commands

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

Examples
Example 1 - Set the maximum number of kilobits per second of Broadcast traffic on port 1 to 10000.

switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)#smartport storm-control broadcast level kpbs 10000

Example 2 - Set the maximum percentage of kilobits per second of Broadcast traffic on port 1 to 30%.

switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)#smartport storm-control broadcast level 30

35.19 smartport storm-control include-multicast
Use the smartport storm-control include-multicast Interface Configuration mode command to count Multicast packets in a Broadcast storm control. Use the no form of this command to disable counting of Multicast packets in the Broadcast storm control.

Syntax
smartport storm-control include-multicast [unknown-unicast]
no smartport storm-control include-multicast

Parameters
unknown-unicast—Specifies also the count of unknown Unicast packets.

Default Configuration
Disabled

Command Mode
Interface Configuration mode (Ethernet)
Example

switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# smartport storm-control include-multicast
36.1 cdp run

The `cdp run` Global Configuration mode command enables CDP globally. The `no` format of this command disabled CDP globally.

Syntax

cdp run

no cdp run

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

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

To learn and advertise CDP information, it must be globally enabled (it is so by default) and also enabled on interfaces (also by default).

Example
36.2 cdp enable

The `cdp enable` Interface Configuration mode command enables CDP on interface. The `no` format of the CLI command disables CDP on an interface.

**Syntax**

```
cdp enable
```

**Parameters**

N/A

**Default Configuration**

Enabled

**Command Mode**

Ethernet Interface

**User Guidelines**

For CDP to be enabled on an interface, it must first be enabled globally using `cdp run`.

**Example**

```
switchxxxxxx(config) cdp run
switchxxxxxx(config) interface gi1
switchxxxxxx(config-if) cdp enable
```

36.3 cdp pdu

Use the `cdp pdu` Global Configuration mode command when CDP is not enabled globally. It specifies CDP packets handling when CDP is globally disabled. The `no` format of this command returns to default.

**Syntax**

```
cdp pdu [filtering | bridging | flooding]
```
no cdp pdu

Parameters

- **filtering**—Specify that when CDP is globally disabled, CDP packets are filtered (deleted).
- **bridging**—Specify that when CDP is globally disabled, CDP packets are bridged as regular data packets (forwarded based on VLAN).
- **flooding**—Specify that when CDP is globally disabled, CDP packets are flooded to all the ports in the product that are in 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 CDP-disabled ports.

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

Example

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

36.4 cdp advertise-v2

The `cdp advertise-v2` Global Configuration mode command specifies version 2 of transmitted CDP packets. The `no` format of this command specifies version 1.

Syntax

- `cdp advertise-v2`
- `no cdp advertise-v2`
Parameters
N/A

Default Configuration
Version 2.

Command Mode
Global Configuration mode

Example

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

### 36.5 cdp appliance-tlv enable

The `cdp appliance-tlv enable` Global Configuration mode command enables sending of the Appliance TLV. The `no` format of this command disables the sending of the Appliance TLV.

Syntax

- `cdp appliance-tlv enable`
- `no cdp appliance-tlv enable`

Parameters
N/A

Default Configuration
Enabled

Command Mode
Global Configuration mode

User Guidelines

This MIB specifies the Voice VLAN ID (VVID) to which this port belongs:
- **0** - The CDP packets transmitting through this port would contain Appliance VLAN-ID TLV with value of 0. VoIP and related packets are expected to be sent and received with VLAN-id=0 and an 802.1p priority.

- **1..4094** - The CDP packets transmitting through this port would contain Appliance VLAN-ID TLV with N. VoIP and related packets are expected to be sent and received with VLAN-ID=N and an 802.1p priority.

- **4095** - The CDP packets transmitting through this port would contain Appliance VLAN-ID TLV with value of 4095. VoIP and related packets are expected to be sent and received untagged without an 802.1p priority.

- **4096** - The CDP packets transmitting through this port would not include Appliance VLAN-ID TLV; or, if the VVID is not supported on the port, this MIB object will not be configurable and will return 4096.

**Example**

```
switchxxxxxx(config) cdp appliance-tlv enable
```

### 36.6 cdp mandatory-tlvs validation

Use the `cdp mandatory-tlvs validation` Global Configuration mode command to validate that all mandatory (according to CDP protocol) TLVs are present in received CDP frames. The `no` format of this command disables the validation.

If the mandatory TLVs are not included in the packet, it is deleted.

**Syntax**

```
cdp mandatory-tlvs validation
no cdp mandatory-tlvs validation
```

**Parameters**

N/A

**Default Configuration**

Enabled.

**Command Mode**

Global Configuration mode
Example

Turns off mandatory TLV validation:

```
switchxxxxxx(config) no cdp mandatory-tlvs validation
```

### 36.7 cdp source-interface

The `cdp source-interface` Global Configuration mode command specifies the CDP source port used for source IP address selection. The `no` format of this command deletes the source interface.

**Syntax**

```
cdp source-interface interface-id
no cdp source-interface
```

**Parameters**

- `interface-id`—Source port used for Source IP address selection.

**Default Configuration**

No CDP source interface is specified.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the `cdp source-interface` command to specify an interface whose minimal IP address will be advertised in the TVL instead of the minimal IP address of the outgoing interface.

**Example**

```
switchxxxxxx(config) cdp source-interface gi1
```
36.8  cdp log mismatch duplex

Use the **cdp log mismatch duplex** Global and Interface Configuration mode command to enable validating that the duplex status of a port received in a CDP packet matches the ports actual configuration. If not, a SYSLOG duplex mismatch message is generated. The **no** format of the CLI command disables the generation of the SYSLOG messages.

**Syntax**

```plaintext
cdp log mismatch duplex
no cdp log mismatch duplex
```

**Parameters**

N/A

**Default Configuration**

The switch reports duplex mismatches from all ports.

**Command Mode**

Global Configuration mode

Ethernet Interface

**Example**

```plaintext
switchxxxxxx(config) interface gi1
switchxxxxxx(config-if) cdp log mismatch duplex
```

36.9  cdp log mismatch voip

Use the **cdp log mismatch voip** Global and Interface Configuration mode command to enable validating that the VoIP status of the port received in a CDP packet matches its actual configuration. If not, a SYSLOG message is generated by CDP. The **no** format of the CLI command disables the generation of the SYSLOG messages.

**Syntax**

```plaintext
cdp log mismatch voip
```


no cdp log mismatch voip

Parameters
N/A

Default Configuration
The switch reports voip mismatches from all ports.

Command Mode
Global Configuration mode
Ethernet Interface

Example

switchxxxxxx(config) interface gi1
switchxxxxxx(config-if) cdp log mismatch voip

36.10  cdp log mismatch native

Use the cdp log mismatch native Global and Interface Configuration mode command to enable validating that the native VLAN received in a CDP packet matches the actual native VLAN of the port. If not, a SYSLOG native mismatch message is generated. The no format of the CLI command disables the generation of the SYSLOG messages.

Syntax

  cdp log mismatch native
  no cdp log mismatch native

Parameters

N/A

Default Configuration
The switch reports Native VLAN mismatches from all ports.
36.11  cdp device-id format

The `cdp device-id format` Global Configuration mode command specifies the format of the Device-ID TLV. The `no` format of this command returns to default.

Syntax

```
cdp device-id format {mac | serial-number}
no cdp device-id format
```

Parameters

- `mac`—Specifies that the Device-ID TLV contains the device’s MAC address.
- `serial-number`—Specifies that Device-ID TLV contains the device’s hardware serial number.

Default Configuration

MAC address is selected by default.

Command Mode

Global Configuration mode

Example

```plaintext
switchxxxxxx(config) cdp device-id format serial-number
```
36.12 cdp timer

The `cdp timer` Global Configuration mode command specifies how often CDP packets are transmitted. The `no` format of this command returns to default.

Syntax

```
cdp timer seconds
no cdp timer
```

Parameters


Default Configuration

60 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config) cdp timer 100
```

36.13 cdp holdtime

The `cdp holdtime` Global Configuration mode command specified a value of the Time-to-Live field into sent CDP messages. The `no` format of this command returns to default.

Syntax

```
cdp holdtime seconds
no cdp timer
```

Parameters

- `seconds`—Value of the Time-to-Live field in seconds. The value should be bigger than the value of Transmission Timer.
Parameters range

seconds—10 - 255.

Default Configuration
180 seconds.

Command Mode
Global Configuration mode

Example

switchxxxxxx(config)  cdp  holdtime  100

36.14 clear cdp counters

The clear cdp counters Global Configuration mode command resets the CDP traffic counters to 0.

Syntax

clear cdp counters

Parameters
N/A

Command Mode
Global Configuration mode

Example

switchxxxxxx(config)  clear  cdp  counters

36.15 clear cdp table

The clear cdp table Global Configuration mode command deletes the CDP Cache tables.
### Syntax

clear cdp table

### Parameters
N/A

### Command Mode
Global Configuration mode

### Example

```
switchxxxxxx(config) clear cdp table
```

36.16 show cdp

The `show cdp` Privileged EXEC mode command displays the interval between advertisements, the number of seconds the advertisements are valid and version of the advertisements.

### Syntax

show cdp

### Parameters
N/A

### Command Mode
Privileged EXEC mode

### Example

```
switch>show cdp
Global CDP information:
      cdp is globally enabled
      cdp log duplex mismatch is globally enabled
      cdp log voice VLAN mismatch is globally enabled
      cdp log native VLAN mismatch is globally disabled
Mandatory TLVs are
      Device-ID TLV (0x0001
```
Address TLV (0x0002)
Port-ID TLV (0x0003)
Capabilities TLV (0x0004)
Version TLV (0x0005)
Platform TLV (0x0006)

Sending CDPv2 advertisements is enabled
Sending Appliance TLV is enabled
Device ID format is Serial Number
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds

36.17  show cdp entry

The **show cdp entry** Privileged EXEC mode command displays information about specific neighbor. Display can be limited to protocol or version information.

**Syntax**

```
show cdp entry {* | device-name}[protocol | version]
```

**Parameters**

- `*`—Specifies all neighbors
- `device-name`—Specifies the name of the neighbor.
- `protocol`—Limits the display to information about the protocols enabled on neighbors.
- `version`—Limits the display to information about the version of software running on the neighbors.

**Default Configuration**

Version

**Command Mode**

Privileged EXEC mode

**Example**

```
switchxxxxxx#show cdp entry device.cisco.com
Device ID: device.cisco.com
```
Advertisement version: 2
Entry address(es):
  IP address: 192.168.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1
Platform: cisco 4500, Capabilities: Router
Interface: gi1, Port ID (outgoing port): Ethernet0
Holdtime: 125 sec
Version:
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M), Version 11.1(10.4), MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by dschwart

switchxxxxxx#show cdp entry device.cisco.com
Protocol information for device.cisco.com:
  IP address: 192.168.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1

switchxxxxxx#show cdp entry device.cisco.com version
Version information for device.cisco.com:
  Cisco Internetwork Operating System Software
  IOS (tm) 4500 Software (C4500-J-M), Version 11.1(10.4), MAINTENANCE INTERIM SOFTWARE
  Compiled Mon 07-Apr-97 19:51 by dschwart

36.18  show cdp interface

The show cdp interface Privileged EXEC mode command displays information about ports on which CDP is enabled.

Syntax

    show cdp interface interface-id
Parameters

interface-id—Port ID.

Command Mode

Privileged EXEC mode

Example

switchxxxxxx#show cdp interface gi1
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 disabled
  Per interface is enabled
gi1 is Down, CDP is enabled
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

36.19 show cdp neighbors

The show cdp neighbors Privileged EXEC mode command displays information about neighbors kept in the main or secondary cache.

Syntax

show cdp neighbors [interface-id] [detail | secondary]

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.
- **secondary**—Displays information about neighbors from the secondary cache.

**Default Configuration**

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

If detail or secondary are not specified, the default is secondary.

**Command Mode**

Privileged EXEC mode

**Example**

```
switchxxxxxx# show cdp neighbors
```

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

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

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local</th>
<th>Adv</th>
<th>Time To Capability</th>
<th>Platform</th>
<th>Port ID</th>
<th>Interface</th>
<th>Ver.</th>
<th>Live</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTK-SW-A-86.marvel</td>
<td>gi48</td>
<td>2</td>
<td>147</td>
<td>S I</td>
<td>cisco</td>
<td>GigabitEth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>l.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WS-C4510R-E</td>
<td>rnet3/39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESW-520-8P</td>
<td>gi48</td>
<td>2</td>
<td>153</td>
<td>S I M</td>
<td>ESW-520-8P</td>
<td>g1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESW-540-8P</td>
<td>gi48</td>
<td>2</td>
<td>146</td>
<td>S I M</td>
<td>ESW-540-8P</td>
<td>g9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>003106131611</td>
<td>gi48</td>
<td>2</td>
<td>143</td>
<td>S I</td>
<td>Cisco</td>
<td>fa2/2/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SG500-28P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(PID:SG500-28P-K9)-VSD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>001828100211</td>
<td>gi48</td>
<td>2</td>
<td>173</td>
<td>S I</td>
<td>Cisco SF</td>
<td>fa20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>200-48P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(PID:SLM248P T)-VSD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c47d4fed9302</td>
<td>gi48</td>
<td>2</td>
<td>137</td>
<td>S I</td>
<td>Cisco SF</td>
<td>fa12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>200-48</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```

switchxxxxxx# show cdp neighbors detail
```
Device ID: lab-7206
Advertisement version: 2
Entry address(es):
   IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): fa1/1/0
Time To Live: 123 sec
Version:
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
Duplex: half

-------------------------
Device ID: lab-as5300-1
Entry address(es):
   IP address: 172.19.169.87
Platform: cisco AS5300, Capabilities: Router
Device ID: SEP000427D400ED
Advertisement version: 2
Entry address(es):
   IP address: 1.6.1.81
Platform: Cisco IP Phone 7940, Capabilities: Host
Interface: fa1/1/1, Port ID (outgoing port): Port 1
Time To Live: 150 sec
Version:
P00303020204
Duplex: full
sysName: a-switch
Power drawn: 6.300 Watts
### Command: `show cdp neighbors secondary`

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

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>Mac Address</th>
<th>TimeToLive</th>
<th>Capability</th>
<th>VLAN-ID</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa1/1/1</td>
<td>00:00:01:23a:86:9c</td>
<td>157</td>
<td>R,S</td>
<td>10</td>
<td>206VXRYC</td>
</tr>
<tr>
<td>fa1/1/1</td>
<td>00:00:05:53a:86:9c</td>
<td>163</td>
<td>R,S</td>
<td>10</td>
<td>ABCD-VSD</td>
</tr>
<tr>
<td>fa1/1/3</td>
<td>00:00:01:23b:86:9c</td>
<td>140</td>
<td>R</td>
<td></td>
<td>QACSZ</td>
</tr>
<tr>
<td>fa1/1/3</td>
<td>00:00:ab:c2a:86:9c</td>
<td>132</td>
<td>T</td>
<td></td>
<td>CAT3000</td>
</tr>
</tbody>
</table>

### Field Definitions:

- **Advertisement version**—The version of CDP being used for CDP advertisements.
- **Capabilities**—The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
- **COS for Untrusted Ports**—The COS value with which all packets received on an untrusted port should be marked by a simple switching device which cannot itself classify individual packets.
- **Device ID**—The name of the neighbor device and either the MAC address or the serial number of this device.
- **Duplex**—The duplex state of connection between the current device and the neighbor device.
- **Entry address(es)**—A list of network addresses of neighbor devices.
- **Extended Trust**—The Extended Trust.
- **External Port-ID**—Identifies the physical connector port on which the CDP packet is transmitted. It is used in devices, such as those with optical ports, in which signals from multiple hardware interfaces are multiplexed through a single physical port. It contains the name of the external physical port through which the multiplexed signal is transmitted.
- **Interface**—The protocol and port number of the port on the current device.
- **IP Network Prefix**—It is used by On Demand Routing (ODR). When transmitted by a hub router, it is a default route (an IP address). When
transmitted by a stub router, it is a list of network prefixes of stub networks to which the sending stub router can forward IP packets.

- **Management Address**—When present, it contains a list of all the addresses at which the device will accept SNMP messages, including those it will only accept when received on interface(s) other than the one over which the CDP packet is being sent.

- **MTU**—The MTU of the interface via which the CDP packet is sent.

- **Native VLAN**—The ID number of the VLAN on the neighbor device.

- **Physical Location**—A character string indicating the physical location of a connector which is on, or physically connected to, the interface over which the CDP packet containing this TLV is sent.

- **Platform**—The product name and number of the neighbor device. In the case of the Secondary Cache only the 8 last characters of the value are printed.

- **Power Available**—Every switch interface transmits information in the Power Available TLV, which permits a device which needs power to negotiate and select an appropriate power setting. The Power Available TLV includes four fields.

- **Power Consumption**—The maximum amount of power, in milliwatts, expected to be obtained and consumed from the interface over which the CDP packet is sent.

- **Power Drawn**—The maximum requested power.

  Note: For IP Phones the value shown is the maximum requested power (6.3 Watts). This value can be different than the actual power supplied by the routing device (generally 5 watts; shown using the show power command).

- **Protocol-Hello**—Specifies that a particular protocol has asked CDP to piggyback its "hello" messages within transmitted CDP packets.

- **Remote Port_ID**—Identifies the port the CDP packet is sent on

- **sysName**—An ASCII string containing the same value as the sending device's sysName MIB object.

- **sysObjectId**—The OBJECT-IDENTIFIER value of the sending device's sysObjectId MIB object.
- **Time To Live**—The remaining amount of time, in seconds, the current device will hold the CDP advertisement from a transmitting router before discarding it.
- **Version**—The software version running on the neighbor device.
- **Voice VLAN-ID**—The Voice VLAN-ID.
- **VTP Management Domain**—A string that is the name of the collective group of VLANs associated with the neighbor device.

### 36.20 show cdp tlv

The `show cdp tlv` Privileged EXEC mode command displays information about TLVs sent by CDP on all ports or on a specific port.

**Syntax**

```
show cdp tlv [interface-id]
```

**Parameters**

- `interface-id`—Port ID.

**Default Configuration**

TLVs for all ports.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

You can use the `show cdp tlv` command to verify the TLVs configured to be sent in CDP packets. The `show cdp tlv` command displays information for a single port if specified or for all ports if not specified. Information for a port is displayed if only CDP is really running on the port, i.e. CDP is enabled globally and on the port, which is UP.

**Examples**

**Example 1** - In this example, CDP is disabled and no information is displayed.

```bash
switchxxxxxx#show cdp tlv
```
cdp globally is disabled

---

**Example 2** - In this example, CDP is globally enabled but disabled on the port and no information is displayed.

```
switchxxxxxx#show cdp tlv gi2
```

cdp globally is enabled

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
Interface TLV: gi2
CDP is disabled on gi2

---

**Example 3** - In this example, CDP is globally enabled and enabled on the port, but the port is down and no information is displayed.

```
switchxxxxxx#show cdp tlv interface gi2
```

cdp globally is enabled

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
Interface TLV: gi3
CDP is enabled on gi3
Ethernet gi3 is down

---

**Example 4** - In this example, CDP is globally enabled and enabled on the port, which is up and information is displayed.

```
switchxxxxxx#show cdp tlv interface gi1
```

cdp globally is enabled
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

Interface TLV: gi1
CDP is enabled
Ethernet gi1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4: 1.2.2.2 IPv6:
Port_ID TLV: gi1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
Power Available TLV: Request-ID is 1 Power management-ID is 1;
Available-Power is 10;
Management-Power-Level is 0xFFFFFFFF

Example 5 - In this example, CDP is globally enabled, and no ports are specified, so information is displayed for all ports on which CDP is enabled who are up.

switchxxxxxx# show cdp tlv interface
cdp globally is enabled

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
Interface TLV: gi1
CDP is enabled
Ethernet gi1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4: 1.2.2.2 IPv6:
Port_ID TLV: gi1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
Power Available TLV: Request-ID is 1 Power management-ID is 1;
  Available-Power is 10;
  Management-Power-Level is 0xFFFFFFFF

Interface TLV: gi2
CDP is disabled on gi2
Interface TLV: gi3
CDP is enabled on gi3
Ethernet gi3 is down

36.21 show cdp traffic

The show cdp traffic Privileged EXEC mode command displays the CDP counters, including the number of packets sent and received and checksum errors.

Syntax

show cdp traffic [global | interface-id]

Parameters

- global—Display only the global counters
- **interface-id**—Port for which counters should be displayed.

### Default Configuration

If interface-id is not specified, global counters are displayed for all ports on which CDP is enabled and who are up.

### Command Mode

Privileged EXEC mode

### User Guidelines

Use the `show cdp traffic global` to display only the global counters. Use the `show cdp traffic interface-id` command to display the counters of the given port. Use the command `show cdp traffic` without parameters to display all the counters.

### Example

```
switchxxxxxx#show cdp traffic

CDP Global counters:
    Total packets output: 81684, Input: 81790  
    Hdr syntax: 0, Chksum error: 0, Encaps: 0  
    No memory: 0, Invalid packet: 0  
    CDP version 1 advertisements output: 100, Input 0  
    CDP version 2 advertisements output: 81784, Input 0

fastethernet 1/1/1
    Total packets output: 81684, Input: 81790  
    Hdr syntax: 0, Chksum error: 0, Encaps: 0  
    No memory: 0, Invalid packet: 0  
    CDP version 1 advertisements output: 100, Input 0  
    CDP version 2 advertisements output: 81784, Input 0

fastethernet 1/1/2
    Total packets output: 81684, Input: 81790  
    Hdr syntax: 0, Chksum error: 0, Encaps: 0  
    No memory: 0, Invalid packet: 0  
    CDP version 1 advertisements output: 100, Input 0
```
CDP version 2 advertisements output:  81784, Input  0

Field Definition:

- **Total packets output**—The number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.

- **Input**—The number of CDP advertisements received by the local device. Note that this value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.

- **Hdr syntax**—The number of CDP advertisements with bad headers, received by the local device.

- **Chksum error**—The number of times the checksum (verifying) operation failed on incoming CDP advertisements.

- **No memory**—The number of times the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.

- **Invalid**—The number of invalid CDP advertisements received.

- **CDP version**—Advertisements output The number of CDP Version 1 advertisements sent by the local device.

- **CDP version 1 advertisements Input**—The number of CDP Version 1 advertisements received by the local device.

- **CDP version 2 advertisements output**—The number of CDP Version 2 advertisements sent by the local device.

- **CDP version 2 advertisements Input**—The number of CDP Version 2 advertisements received by the local device.
Link Layer Discovery Protocol (LLDP) Commands

37.1 lldp run

Use the lldp run Global Configuration mode command to enable LLDP. To disable LLDP, use the no form of this command.

Syntax
lldp run
no lldp run

Parameters
N/A.

Default Configuration
Enabled

Command Mode
Global Configuration mode

Example

switchxxxxxx(config)# lldp run

37.2 lldp transmit

Use the lldp transmit Interface Configuration mode command to enable transmitting LLDP on an interface. Use the no form of this command to stop transmitting LLDP on an interface.

Syntax
lldp transmit
no lldp transmit
Parameters
N/A

Default Configuration
Enabled

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. I.e. LLDP frames are sent on 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 transmit
```

## 37.3 lldp receive

Use the `lldp receive` Interface Configuration mode command to enable receiving LLDP on an interface. Use the `no` form of this command to stop receiving LLDP on an interface.

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 LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are received on 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
```

37.4 Ildp timer

Use the `lldp timer` Global Configuration mode command to specify how often the software sends LLDP updates. Use the `no` form of this command to restore the default configuration.

Syntax

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

Parameters

```
timer seconds—Specifies, in seconds, how often the software sends LLDP updates (range: 5-32768 seconds).
```

Default Configuration

30 seconds.

Command Mode

Global Configuration mode
Example

The following example sets the interval for sending LLDP updates to 60 seconds.

```
switchxxxxx(config)# lldp timer 60
```

37.5 lldp hold-multiplier

Use the `lldp hold-multiplier` Global Configuration mode command to specify how long the receiving device holds a LLDP packet before discarding it. Use the `no` form of this command to restore the default configuration.

Syntax

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

Parameters

`hold-multiplier number`—Specifies the LLDP packet hold time interval as a multiple of the LLDP timer value (range: 2-10).

Default Configuration

The default LLDP hold multiplier is 4.

Command Mode

Global Configuration mode

User Guidelines

The actual Time-To-Live (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 hold multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.
Example

The following example sets the LLDP packet hold time interval to 90 seconds.

```
switchxxxxxx(config)# lldp timer 30
switchxxxxxx(config)# lldp hold-multiplier 3
```

### 37.6 lldp reinit

Use the `lldp reinit` Global Configuration mode command to specify the minimum time an LLDP port waits before reinitializing LLDP transmission. Use the `no` form of this command to revert to the default setting.

**Syntax**

`lldp reinit seconds`

`no lldp reinit`

**Parameters**

`reinit seconds`—Specifies the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission. (Range: 1–10)

**Default Configuration**

2 seconds

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# lldp reinit 4
```

### 37.7 lldp tx-delay

Use the `lldp tx-delay` Global Configuration mode command to set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Use the `no` form of this command to restore the default configuration.
Syntax

`lldp tx-delay seconds`

`no lldp tx-delay`

Parameters

`tx-delay seconds`—Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB (range: 1-8192 seconds).

Default Configuration

The default LLDP frame transmission delay is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended that the tx-delay be less than 0.25 of the LLDP timer interval.

Example

The following example sets the LLDP transmission delay to 10 seconds.

```
switchxxxxxx(config)# lldp tx-delay 10
```
**Parameters**

- **tlv**—Specifies the TLVs to be included. Available optional TLVs are: 802.1, port-desc, sys-name, sys-desc, sys-cap, 802.1, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size.

- **none**—Clear all optional TLVs from the interface

If the 802.1 protocol is selected, see the command below.

**Default Configuration**

No optional TLV is transmitted.

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example specifies that the port description TLV is transmitted on gi2.

```
switchxxxxx(config)# interface gi2
switchxxxxx(config-if)# lldp optional-tlv port-desc
```

### 37.9  **lldp optional-tlv 802.1**

Use the `lldp optional-tlv` Interface Configuration mode command to specify which optional TLVs to transmit. Use the `no` form of this command to revert to the default setting.

**Syntax**

- `lldp optional-tlv 802.1 pvid` - The PVID is advertised.
- `no lldp optional-tlv 802.1 pvid` - The PVID is not advertised
- `lldp optional-tlv 802.1 ppvid add ppvid` - The Protocol Port VLAN ID (PPVID) is advertised. The PPVID is the PVID that is used depending on the packet's protocol.
- `lldp optional-tlv 802.1 ppvid remove ppvid` - The PPVID is not advertised.
- `lldp optional-tlv 802.1 vlan add vlan-id` - This `vlan-id` is advertised.
- `lldp optional-tlv 802.1 vlan remove vlan-id` - This `vlan-id` is not advertised.
lldp optional-tlv 802.1 protocol add {stp / rstp / mstp / pause / 802.1x / lacp / gvrp} - The protocols selected are advertised.

lldp optional-tlv 802.1 protocol remove {stp / rstp / mstp / pause / 802.1x / lacp / gvrp} - The protocols selected are not advertised.

Parameters

- lldp optional-tlv 802.1 pvid—Advertises the PVID of the port.
- lldp optional-tlv 802.1 ppvid add/remove ppvid—Adds/removes PPVID for advertising. (range: 0–4094). PPVID = 0 indicates that the port is not capable of supporting port and protocol VLANs and/or the port is not enabled with any protocol VLANs.
- add/remove vlan-id—Adds/removes VLAN for advertising (range: 0–4094).
- add/remove {stp / rstp / mstp / pause / 802.1x / lacp / gvrp}—Add specifies to advertise the specified protocols; remove specifies not to advertise the specified protocol.

Default Configuration

No optional TLV is transmitted.

Command Mode

Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# lldp optional-tlv 802.1 protocol add stp
```

### 37.10 lldp management-address

Use the lldp management-address Interface Configuration (Ethernet) mode command to specify the management address advertised by an interface. Use the no form of this command to stop advertising management address information.

Syntax

```
lldp management-address [ip-address / none / automatic [interface-id]]
```

no lldp management-address
Parameters

- **ip-address**—Specifies the static management address to advertise.
- **none**—Specifies that no address is advertised.
- **automatic**—Specifies that the software automatically selects a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses.
- **automatic interface-id**—(Available only when the device is in Layer 3 (router mode)). Specifies that the software automatically selects a management address to advertise from the IP addresses that are configured on the interface ID. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses of the interface. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses of the interface. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN. Note that if the port or port-channel are members in a VLAN that has an IP address, that address is not included because the address is associated with the VLAN.

Default Configuration

No IP address is advertised.

The default advertisement is **automatic**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Each port can advertise one IP address.

Example

The following example sets the LLDP management address advertisement mode to **automatic** on gi2.

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# lldp management-address automatic
```
37.11 lldp notifications

Use the `lldp notifications` Interface Configuration (Ethernet) mode command to enable/disable sending LLDP notifications on an interface. Use the `no` form of this command to restore the default configuration.

**Syntax**

```plaintext
lldp notifications {enable | disable}
no lldp notifications
```

**Parameters**

- `enable`—Enables sending LLDP notifications.
- `disable`—Disables sending LLDP notifications.

**Default Configuration**

Disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example enables sending LLDP notifications on `gi5`.

```plaintext
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# lldp notifications enable
```

37.12 lldp notifications interval

Use the `lldp notifications interval` Global Configuration mode command to configure the maximum transmission rate of LLDP notifications. Use the `no` form of this command to return to the default.

**Syntax**

```plaintext
lldp notifications interval seconds
no lldp notifications interval
```
Parameters

interval seconds—The device does not send more than a single notification in the indicated period (range: 5–3600).

Default Configuration

5 seconds

Command Mode

Global Configuration mode

Example

switchxxxxxxx(config)# lldp notifications interval 10

37.13  lldp lldpdu

The lldp lldpdu Global Configuration mode command defines LLDP packet handling when LLDP is globally disabled. To restore the default configuration, use the no form of this command.

Syntax

lldp lldpdu {filtering | flooding}

no lldp lldpdu

Parameters

- filtering — Specifies that when LLDP is globally disabled, LLDP packets are filtered (deleted).
- flooding — Specifies that when LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces).

Default Configuration

LLDP packets are filtered when LLDP is globally disabled.

Command Mode

Global Configuration mode
User Guidelines

If the STP mode is 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. The 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 LLDP packets. The LLDP packets are flooded to all ports for which the STP state is Forwarding.
- LLDP packets are sent as untagged.

Example

The following example sets the LLDP packet handling mode to Flooding when LLDP is globally disabled.

```
switchxxxxxx(config)# lldp lldpdu flooding
```

37.14  lldp med

Use the lldp med Interface Configuration (Ethernet) mode command to enable or disable LLDP Media Endpoint Discovery (MED) on a port. Use the no form of this command to return to the default state.

Syntax

```
lldp med {enable [tlv ... tlv4] | disable}
```

Parameters

- enable - Enable LLDP MED
• **tlv**—Specifies the TLV that should be included. Available TLVs are: network-policy, location, and poe-pse, inventory. The capabilities TLV is always included if LLDP-MED is enabled.

• **disable** - disable LLDP MED on the port

**Default Configuration**

Enabled with network-policy TLV

**Command Mode**

Interface Configuration (Ethernet) mode

**Example**

The following example enables LLDP MED with the location TLV on gi3.

```bash
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# lldp med enable location
```

**37.15 lldp med notifications topology-change**

Use the `lldp med notifications topology-change` Interface Configuration (Ethernet) mode command to enable sending LLDP MED topology change notifications on a port. Use the `no` form of this command to restore the default configuration.

**Syntax**

lldp med notifications topology-change `{enable | disable}`

no lldp med notifications topology-change

**Parameters**

- **enable**—Enables sending LLDP MED topology change notifications.
- **disable**—Disables sending LLDP MED topology change notifications.

**Default Configuration**

Disable is the default.
Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables sending LLDP MED topology change notifications on gi2.

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# lldp med notifications topology-change enable
```

### 37.16 lldp med fast-start repeat-count

When a port comes up, LLDP can send packets more quickly than usual using its fast-start mechanism.

Use the `lldp med fast-start repeat-count` Global Configuration mode command to configure the number of packets that is sent during the activation of the fast start mechanism. Use the `no` form of this command return to default.

**Syntax**

```
lldp med fast-start repeat-count number
no lldp med fast-start repeat-count
```

**Parameters**

- `repeat-count number`—Specifies the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism. The range is 1-10.

**Default Configuration**

3

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# lldp med fast-start repeat-count 4
```
37.17  lldp med network-policy (global)

Use the lldp med network-policy Global Configuration mode command to define a LLDP MED network policy. For voice applications, it is simpler to use lldp med network-policy voice auto.

The lldp med network-policy command creates the network policy, which is attached to a port by lldp med network-policy (interface).

The network policy defines how LLDP packets are constructed.

Use the no form of this command to remove LLDP MED network policy.

Syntax

lldp med network-policy number application [vlan vlan-id] [vlan-type {tagged | untagged}] [up priority] [dscp value]

no lldp med network-policy number

Parameters

- **number**—Network policy sequential number. The range is 1-32.
- **application**—The name or the number of the primary function of the application defined for this network policy. Available application names are:
  - voice
  - voice-signaling
  - guest-voice
  - guest-voice-signaling
  - softphone-voice
  - video-conferencing
  - streaming-video
  - video-signaling.
- **vlan vlan-id**—VLAN identifier for the application.
- **vlan-type**—Specifies if the application is using a tagged or an untagged VLAN.
- **up priority**—User Priority (Layer 2 priority) to be used for the specified application.
**dscp value**—DSCP value to be used for the specified application.

**Default Configuration**

No network policy is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the `lldp med network-policy` Interface Configuration 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-signalingly application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 voice-signaling vlan 1
  vlan-type untagged up 1 dscp 2
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

### 37.18 lldp med network-policy (interface)

Use the `lldp med network-policy` Interface Configuration (Ethernet) mode command to attach or remove an LLDP MED network policy on a port. Network policies are created in `lldp med network-policy (global)`.

Use the `no` form of this command to remove all the LLDP MED network policies from the port.

**Syntax**

```
lldp med network-policy {add | remove} number
no lldp med network-policy number
```
Parameters

- **number**—Specifies the network policy sequential number. The range is 1-32
- **add/remove number**—Attaches/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 port, only one network policy per application (voice, voice-signaling, etc.) can be defined.

Example

This example creates a network policy for the voice-signaling application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 voice-signaling vlan 1
  vlan-type untagged up 1 dscp 2
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

### 37.19  **lldp med network-policy voice auto**

A network policy for voice LLDP packets can be created by using the `lldp med network-policy (global)`. The `lldp med network-policy voice auto` Global Configuration mode is simpler in that it uses the configuration of the Voice application to create the network policy instead of the user having to manually configure it.

This command generates an LLDP MED network policy for voice, if the voice VLAN operation mode is auto voice VLAN. The voice VLAN, 802.1p priority, and the DSCP of the voice VLAN are used in the policy. Use the no form of this command
to disable this mode. The network policy is attached automatically to the voice VLAN.

Syntax

```markdown
lldp med network-policy voice auto
no lldp med network-policy voice auto
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

In Auto mode, the Voice VLAN feature determines on which interfaces to advertise the network policy TLV with application type voice, and controls the parameters of that TLV.

To enable the auto generation of a network policy based on the auto voice VLAN, there must be no manual pre-configured network policies for the voice application.

In Auto mode, you cannot manually define a network policy for the voice application using the `lldp med network-policy (global)` command.

Example

```
switchxxxxxxx(config)# lldp med network-policy voice auto
```

### 37.20 clear lldp table

Use the `clear lldp table` command in Privileged EXEC mode to clear the neighbors table for all ports or for a specific port.

Syntax

```
clear lldp table [interface-id]
```
Parameters

interface-id—Specifies a port ID.

Default Configuration

If no interface is specified, the default is to clear the LLDP table for all ports.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxx# clear lldp table gi1
```

### 37.21 lldp med location

Use the lldp med location Interface Configuration (Ethernet) mode command to configure the location information for the LLDP Media Endpoint Discovery (MED) for a port. Use the no form of this command to delete location information for a port.

**Syntax**

```
llaep med location {{coordinate data} | {civic-address data} | {ecs-elin data}}
```

**Parameters**

- **coordinate data**—Specifies the location data as coordinates in hexadecimal format.
- **civic-address data**—Specifies the location data as a civic address in hexadecimal format.
- **ecs-elin data**—Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN) in hexadecimal format.
- **data**—Specifies the location data in the format defined in ANSI/TIA 1057: dotted hexadecimal data: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. (Length: coordinate: 16 bytes. Civic-address: 6-160 bytes. Ecs-elin: 10-25 bytes)
Default Configuration
The location is not configured.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example configures the LLDP MED location information on gi2 as a civic address.

```
switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# lldp med location civic-address 616263646566
```

### 37.22 show lldp configuration

Use the `show lldp configuration` Privileged EXEC mode command to display the LLDP configuration for all ports or for a specific port.

**Syntax**

```
show lldp configuration [interface-id | detailed]
```

**Parameters**

- `interface-id`—Specifies the port ID.
- `detailed`—Displays information for non-present ports in addition to present ports.

**Default Configuration**

Display for all ports. If detailed is not used, only present ports are displayed.

**Command Mode**

Privileged EXEC mode

**Examples**

**Example 1** - Display LLDP configuration for all ports.
Switch# show lldp configuration

State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Optional TLVs</th>
<th>Address</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>172.16.1.1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi2</td>
<td>TX</td>
<td>PD, SN</td>
<td>172.16.1.1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi3</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi5</td>
<td>RX, TX</td>
<td>D, SN, SD, SC</td>
<td>automatic</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi6</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>auto vlan 1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi7</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>auto g1</td>
<td>Disabled</td>
</tr>
<tr>
<td>gi8</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>auto ch1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Example 2 - Display LLDP configuration for port 1.**

Switch# show lldp configuration gi1

State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Optional TLVs</th>
<th>Address</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>72.16.1.1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size

802.1 optional TLVs

PVID: Enabled

PPVIDs: 0, 1, 92

VLANs: 1, 92

Protocols: 802.1x

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer</td>
<td>The time interval between LLDP updates.</td>
</tr>
<tr>
<td>Hold multiplier</td>
<td>The amount of time (as a multiple of the timer interval) that the receiving device holds a LLDP packet before discarding it.</td>
</tr>
<tr>
<td>Reinit timer</td>
<td>The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.</td>
</tr>
<tr>
<td>Tx delay</td>
<td>The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>State</td>
<td>The port’s LLDP state.</td>
</tr>
<tr>
<td>Optional TLVs</td>
<td>Optional TLVs that are advertised. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>PD - Port description</td>
</tr>
<tr>
<td></td>
<td>SN - System name</td>
</tr>
<tr>
<td></td>
<td>SD - System description</td>
</tr>
<tr>
<td></td>
<td>SC - System capabilities</td>
</tr>
<tr>
<td>Address</td>
<td>The management address that is advertised.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Indicates whether LLDP notifications are enabled or disabled.</td>
</tr>
<tr>
<td>PVID</td>
<td>Port VLAN ID advertised.</td>
</tr>
<tr>
<td>PPVID</td>
<td>Protocol Port VLAN ID advertised.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Protocols advertised.</td>
</tr>
</tbody>
</table>
37.23 show lldp med configuration

Use the `show lldp med configuration` Privileged EXEC mode command to display the LLDP Media Endpoint Discovery (MED) configuration for all ports or for a specific port.

Syntax

```
show lldp med configuration [interface-id | detailed]
```

Parameters

- `interface-id`—Specifies the port ID.
- `detailed`—Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

**Example 1** - The following example displays the LLDP MED configuration for all interfaces.

```
switchxxxxxx# show lldp med configuration
Fast Start Repeat Count: 4.
lldp med network-policy voice: manual
Network policy 1
--------------
Application type: voiceSignaling
VLAN ID: 1 untagged
Layer 2 priority: 0
DSCP: 0
```
### Example 2 - The following example displays the LLDP MED configuration for gi1.

```
switchxxxxxx# show lldp med configuration gi1
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Capabilities</th>
<th>Network Policy</th>
<th>Location</th>
<th>Notifications</th>
<th>Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Network policies:
Location:

### 37.24 show lldp local tlvs-overloading

When an LLDP packet contains too much information for one packet, this is called overloading. Use the `show lldp local tlvs-overloading` EXEC mode command to display the status of TLVs overloading of the LLDP on all ports or on a specific port.

**Syntax**

```
show lldp local tlvs-overloading [interface-id]
```

**Parameters**

- `interface-id`—Specifies a port ID.

**Default Configuration**

If no port ID is entered, the command displays information for all ports.
Command Mode

EXEC mode

User Guidelines

The command calculates the overloading status of the current LLDP configuration, and not for the last LLDP packet that was sent.

Example

```
Switch# show lldp local tlvs-overloading gi1

<table>
<thead>
<tr>
<th>TLVs Group</th>
<th>Bytes</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory</td>
<td>31</td>
<td>Transmitted</td>
</tr>
<tr>
<td>LLDP-MED Capabilities</td>
<td>9</td>
<td>Transmitted</td>
</tr>
<tr>
<td>LLDP-MED Location</td>
<td>200</td>
<td>Transmitted</td>
</tr>
<tr>
<td>802.1</td>
<td>1360</td>
<td>Overloading</td>
</tr>
</tbody>
</table>

Total: 1600 bytes
Left: 100 bytes
```

37.25 show lldp local

Use the `show lldp local` Privileged EXEC mode command to display the LLDP information that is advertised from a specific port.

Syntax

```
show lldp local interface-id
```

Parameters

```
interface-id—Specifies a port ID.
```

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode
Example

The following examples display LLDP information that is advertised from gi1 and 2.

Switch# show lldp local gi1
Device ID: 0060.704C.73FF
Port ID: gi1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Hardware Revision: B1
Firmware Revision: A1
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1
Asset ID: Asset 123
Switch# show lldp local gi2
LLDP is disabled.

37.26 show lldp statistics

Use the show lldp statistics EXEC mode command to display LLDP statistics on all ports or a specific port.
Syntax

show lldp statistics [interface-id | detailed]

Parameters

- **interface-id**—Specifies the port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

```
switchxxxxxx# show lldp statistics

Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>TX Frames</th>
<th>RX Frame</th>
<th>RX TLVs</th>
<th>RX Ageouts</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>730</td>
<td>850</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi3</td>
<td>730</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi6</td>
<td>8</td>
<td>7</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>gi7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi9</td>
<td>730</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
37.27  show lldp neighbors

Use the show lldp neighbors Privileged EXEC mode command to display information about neighboring devices discovered using LLDP. The information can be displayed for all ports or for a specific port.

Syntax

show lldp neighbors [interface-id] [detail | secondary]

Parameters

- **interface-id**—Specifies a port ID.
- **detail**—Displays detailed information about a neighbor (or neighbors) from the main cache.
- **secondary**—Displays information about neighbors from the secondary cache.

Default Configuration

If no port ID is entered, the command displays information for all ports. Detail is the default parameter.

Command Mode

Privileged EXEC mode

User Guidelines

A TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

Examples

Example 1 - The following example displays information about neighboring devices discovered using LLDP on all ports.

Location information, if it exists, is also displayed.

Switch# show lldp neighbors
Example 2 - The following example displays information about neighboring devices discovered using LLDP port 1.

Switch# show lldp neighbors gi1
Device ID: 00:00:00:11:11:11
Port ID: gi
System Name: ts-7800-2
Capabilities: B
System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex.
Operational MAU type: 1000BaseTFD
802.3 Power via MDI
MDI Power support Port Class: PD
PSE MDI Power Support: Not Supported
PSE MDI Power State: Not Enabled
PSE power pair control ability: Not supported.
PSE Power Pair: Signal
PSE Power class: 1

802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
802.3 EEE
Remote Tx: 25 usec
Remote Rx: 30 usec
Local Tx Echo: 30 usec
Local Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.
LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9
LLDP-MED Location

The following table describes significant LLDP fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The neighbor device’s configured ID (name) or MAC address.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The neighbor device’s port ID.</td>
</tr>
<tr>
<td>System name</td>
<td>The neighbor device’s administratively assigned name.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>The capabilities discovered on the neighbor device. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>B - Bridge</td>
</tr>
<tr>
<td></td>
<td>R - Router</td>
</tr>
<tr>
<td></td>
<td>W - WLAN Access Point</td>
</tr>
<tr>
<td></td>
<td>T - Telephone</td>
</tr>
<tr>
<td></td>
<td>D - DOCSIS cable device</td>
</tr>
<tr>
<td></td>
<td>H - Host</td>
</tr>
<tr>
<td></td>
<td>r - Repeater</td>
</tr>
<tr>
<td></td>
<td>O - Other</td>
</tr>
<tr>
<td>System description</td>
<td>The neighbor device’s system description.</td>
</tr>
<tr>
<td>Port description</td>
<td>The neighbor device’s port description.</td>
</tr>
<tr>
<td>Management address</td>
<td>The neighbor device’s management address.</td>
</tr>
<tr>
<td>Auto-negotiation support</td>
<td>The auto-negotiation support status on the port. (Supported or Not Supported)</td>
</tr>
<tr>
<td>Auto-negotiation status</td>
<td>The active status of auto-negotiation on the port. (Enabled or Disabled)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auto-negotiation</td>
<td>The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.</td>
</tr>
<tr>
<td>Advertised Capabilities</td>
<td></td>
</tr>
<tr>
<td>Operational MAU type</td>
<td>The port MAU type.</td>
</tr>
<tr>
<td>LLDP MED</td>
<td></td>
</tr>
<tr>
<td>Capabilities</td>
<td>The sender's LLDP-MED capabilities.</td>
</tr>
<tr>
<td>Device type</td>
<td>The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.</td>
</tr>
<tr>
<td>LLDP MED - Network Policy</td>
<td></td>
</tr>
<tr>
<td>Application type</td>
<td>The primary function of the application defined for this network policy.</td>
</tr>
<tr>
<td>Flags</td>
<td>Flags. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>Unknown policy: Policy is required by the device, but is currently unknown.</td>
</tr>
<tr>
<td></td>
<td>Tagged VLAN: The specified application type is using a Tagged VLAN.</td>
</tr>
<tr>
<td></td>
<td>Untagged VLAN: The specified application type is using an Untagged VLAN.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier for the application.</td>
</tr>
<tr>
<td>Layer 2 priority</td>
<td>The Layer 2 priority used for the specified application.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The DSCP value used for the specified application.</td>
</tr>
<tr>
<td>LLDP MED - Power Over Ethernet</td>
<td></td>
</tr>
<tr>
<td>Power type</td>
<td>The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).</td>
</tr>
<tr>
<td>Power Source</td>
<td>The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Power priority</td>
<td>The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.</td>
</tr>
<tr>
<td>Power value</td>
<td>The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.</td>
</tr>
<tr>
<td>LLDP MED - Location</td>
<td></td>
</tr>
<tr>
<td>Coordinates, Civic address, ECS ELIN.</td>
<td>The location information raw data.</td>
</tr>
</tbody>
</table>
38.1 ip igmp snooping (Global)

Use the ip igmp snooping Global Configuration mode command to enable Internet Group Management Protocol (IGMP) snooping. Use the no form of this command to disable IGMP snooping.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables IGMP snooping.

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

38.2 ip igmp snooping vlan

Use the ip igmp snooping vlan Global Configuration mode command to enable IGMP snooping on a specific VLAN. Use the no form of this command to disable IGMP snooping on a VLAN interface.

Syntax

ip igmp snooping vlan vlan-id

no ip igmp snooping vlan vlan-id
Parameters

\texttt{vlan \textit{vlan-id}}—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2 and IGMPv3 are supported.

To activate IGMP snooping, the \texttt{bridge multicast filtering} should be enabled.

The user guidelines of the \texttt{bridge multicast mode} Interface VLAN Configuration command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

### 38.3 ip igmp snooping vlan mrouter

Use the \texttt{ip igmp snooping vlan mrouter} Global Configuration mode command to enable automatic learning of Multicast router ports on a VLAN. Use the \texttt{no} form of this command to remove the configuration.

Syntax

\texttt{ip igmp snooping vlan \textit{vlan-id} mrouter learn pim-dvmrp}

\texttt{no ip igmp snooping vlan \textit{vlan-id} mrouter learn pim-dvmrp}

Parameters

\texttt{vlan \textit{vlan-id}}—Specifies the VLAN.

Default Configuration

Learning \texttt{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
- MRDISC 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
```

38.4 ip igmp snooping vlan mrouter interface

Use the `ip igmp snooping mrouter interface` Global Configuration mode command to define a port that is connected to a Multicast router port. Use the `no` form of this command to remove the configuration.

Syntax

```
ip igmp snooping vlan vlan-id mrouter interface interface-list
no ip igmp snooping vlan vlan-id mrouter interface interface-list
```

Parameters

- `vlan vlan-id`—Specifies the VLAN.
- `interface interface-list`—Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No ports defined
Command Mode
Global Configuration mode

User Guidelines
A port that is defined as a Multicast router port receives all IGMP packets (reports and queries) as well as all Multicast data.
You can execute the command before the VLAN is created.

Example

switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter interface gi1

38.5 ip igmp snooping vlan forbidden mrouter
Use the ip igmp snooping vlan forbidden mrouter Global Configuration mode command to forbid a port from being defined as a Multicast router port by static configuration or by automatic learning. Use the no form of this command to remove the configuration.

Syntax
ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list
no ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list

Parameters

- vlan vlan-id—Specifies the VLAN.
- interface interface-list—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration
No ports defined.

Command Mode
Global Configuration mode
User Guidelines

A port that is a forbidden mrouter port cannot be a Multicast router port (i.e. 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 interface gi1
```

38.6 ip igmp snooping vlan static

Use the `ip igmp snooping vlan static` Global Configuration mode command to register an IP-layer Multicast address to the bridge table, and to add static ports to the group defined by this address. Use the `no` form of this command to remove ports specified as members of a static Multicast group.

Syntax

```
ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
no ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
```

Parameter

- `vlan vlan-id`—Specifies the VLAN.
- `static ip-address`—Specifies the IP Multicast address.
- `interface interface-list`—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

Static Multicast addresses can only be defined on static VLANs.

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

```
switchxxxxx(config)# ip igmp snooping vlan 1 static 239.2.2.2 interface gi1
```

### 38.7 ip igmp snooping vlan multicast-tv

Use the `ip igmp snooping vlan multicast-tv` Global Configuration mode command to define the Multicast IP addresses that are associated with a Multicast TV VLAN. Use the no form of this command to remove all associations.

**Syntax**

```
ip igmp snooping vlan vlan-id multicast-tv ip-multicast-address [count number]
no ip igmp snooping vlan vlan-id multicast-tv ip-multicast-address [count number]
```

**Parameters**

- `vlan-id`—Specifies the VLAN
- `count number`—Configures multiple contiguous Multicast IP addresses. If not specified, the default is 1. (Range: 1–256)

**Default Configuration**

No Multicast IP address is associated.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use this command to define the Multicast transmissions on a Multicast-TV VLAN. The configuration is only relevant for an Access port that is a member in the configured VLAN as a Multicast-TV VLAN.

If an IGMP message is received on such an Access port, it is associated with the Multicast-TV VLAN only if it is for one of the Multicast IP addresses that are associated with the Multicast-TV VLAN.

Up to 256 VLANs can be configured.
Example

switchxxxxxx(config)# ip igmp snooping vlan 1 multicast-tv 239.2.2.2 count 3

38.8 ip igmp snooping map cpe vlan

The `ip igmp snooping map cpe vlan` Global Configuration mode command maps CPE VLANs to Multicast-TV VLANs. Use the `no` form of this command to remove the mapping.

Syntax

`ip igmp snooping map cpe vlan  vlan-id  multicast-tv vlan  vlan-id`

`no ip igmp snooping map cpe vlan  vlan-id`

Parameters

- `cpe vlan  vlan-id`—Specifies the CPE VLAN ID.
- `multicast-tv vlan  vlan-id`—Specifies the Multicast-TV VLAN ID.

Default Configuration

No mapping exists.

Command Mode

Global Configuration mode

User Guidelines

Use this command to associate the CPE VLAN with a Multicast-TV VLAN.

If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is mapping from that CPE VLAN to a Multicast-TV VLAN, the IGMP message is associated with the Multicast-TV VLAN.

Example

The following example maps CPE VLAN 2 to Multicast-TV VLAN 31.

switchxxxxxx(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan 31
38.9 ip igmp snooping vlan querier

Use the `ip igmp snooping vlan querier` Global Configuration mode command to enable the Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the `no` form of this command to disable the IGMP querier on a VLAN interface.

**Syntax**

```
ip igmp snooping vlan vlan-id querier
no ip igmp snooping vlan vlan-id querier
```

**Parameters**

`vlan vlan-id`—Specifies the VLAN

**Default Configuration**

Disabled

**Command Mode**

Global Configuration mode

**User Guidelines**

The IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN.

At most one switch can be configured as an IGMP Querier for a VLAN.

When the IGMP snooping querier is enabled, it starts after a host-time-out/2 with no IGMP traffic being detected from a Multicast router.

The IGMP Snooping Querier disables itself if it detects IGMP traffic from a Multicast router. It restarts automatically after host-time-out/2.

**Example**

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```
38.10  ip igmp snooping vlan querier address

Use the `ip igmp snooping vlan querier address` Global Configuration mode command to define the source IP address that the IGMP snooping querier uses. Use the `no` form of this command to return to default.

Syntax

```
ip igmp snooping vlan vlan-id querier address ip-address
no ip igmp snooping vlan vlan-id querier address
```

Parameters

- `vlan vlan-id`—Specifies the VLAN.
- `querier address ip-address`—Source IP address.

Default Configuration

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If there are multiple IP addresses, the minimum IP address defined on the VLAN is used.

Command Mode

Global Configuration mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the querier’s VLAN, the querier is disabled.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier address 10.5.234.205
```

38.11  ip igmp snooping vlan querier version

Use the `ip igmp snooping vlan querier version` Global Configuration mode command to configure the IGMP version of an IGMP querier on a specific VLAN. Use the `no` form of this command to return to the default version.
**IGMP Snooping Commands**

**Syntax**

`ip igmp snooping vlan vlan-id querier version {2 | 3}`

`no ip igmp snooping vlan vlan-id querier version`

**Parameters**

- `vlan vlan-id`—Specifies the VLAN.
- `querier version 2`—Specifies that the IGMP version would be IGMPv2.
- `querier version 3`—Specifies that the IGMP version would be IGMPv3.

**Default Configuration**

IGMPv2.

**Command Mode**

Global Configuration mode

**Example**

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

**38.12 ip igmp robustness**

Use the `ip igmp robustness` Interface Configuration (VLAN) mode command to set the IGMP robustness variable on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

`ip igmp robustness count`

`no ip igmp robustness`

**Parameters**

`count`—The number of expected packet loss on a link. Parameter range. (Range: 1–7)

**Default Configuration**

2
**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created, but you must enter the command in Interface VLAN mode.

**Example**

```
switchxxxxx(config)# interface vlan 1
switchxxxxx(config-if)# ip igmp robustness 3
```

### 38.13 ip igmp query-interval

Use the `ip igmp query-interval` Interface Configuration (VLAN) mode command to configure the Query interval on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

```
ip igmp query-interval seconds
no ip igmp query-interval
```

**Parameters**

- `seconds`—Frequency, in seconds, at which IGMP query messages are sent on the interface. (Range: 30–18000)

**Default Configuration**

125

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.
Example

switchxxxxx(config)# interface vlan 1
switchxxxxx(config-if)# ip igmp query-interval 200

### 38.14 ip igmp query-max-response-time

Use the `ip igmp query-max-response-time` Interface Configuration (VLAN) mode command to configure the Query Maximum Response time on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

```
ip igmp query-max-response-time seconds
no ip igmp query-max-response-time
```

**Parameters**

- `seconds`—Maximum response time, in seconds, advertised in IGMP queries.
  (Range: 5–20)

**Default Configuration**

10

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

```
switchxxxxx(config)# interface vlan 1
switchxxxxx(config-if)# ip igmp query-max-response-time 20
```
38.15 ip igmp last-member-query-count

Use the `ip igmp last-member-query-count` Interface Configuration (VLAN) mode command to configure the Last Member Query Counter on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

```plaintext
ip igmp last-member-query-count count
no ip igmp last-member-query-count
```

**Parameter**

`count`—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

**Default Configuration**

A value of Robustness variable

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

You can execute the command before the VLAN is created.

**Example**

```plaintext
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-count 7
```

38.16 ip igmp last-member-query-interval

Use the `ip igmp last-member-query-interval` Interface Configuration (VLAN) mode command to configure the Last Member Query interval on a VLAN. Use the `no` format of the command to return to default.

**Syntax**

```plaintext
ip igmp last-member-query-interval milliseconds
no ip igmp last-member-query-interval
```
Parameters

milliseconds—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500)

Default Configuration

1000

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-interval 2000
```

38.17  ip igmp snooping vlan immediate-leave

Use the `ip igmp snooping vlan immediate-leave` Global Configuration mode command to enable the IGMP Snooping Immediate-Leave processing on a VLAN. Use the `no` format of the command to disable IGMP Snooping Immediate-Leave processing.

Syntax

```
ip igmp snooping vlan vlan-id immediate-leave
no ip igmp snooping vlan vlan-id immediate-leave
```

Parameters

`vlan vlan-id`—Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration

Disabled
Command Mode
Global Configuration mode

User Guidelines
You can execute the command before the VLAN is created.

Example
The following example enables IGMP snooping immediate-leave feature on VLAN 1.

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

38.18  show ip igmp snooping mrouter

The `show ip igmp snooping mrouter` EXEC mode command displays information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN.

Syntax
```
show ip igmp snooping mrouter [interface vlan-id]
```

Parameters
- `interface vlan-id`—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000.

```
switchxxxxxx# show ip igmp snooping mrouter interface 1000

+--------+----------+---------+--------+
| VLAN   | Dynamic  | Static  | Forbidden |
|--------+----------+---------+--------|
| ------ | -------- | ------- | ------ |
| 1000   | gi1      | gi2     | gi3-23 |
```
38.19 show ip igmp snooping interface

The show ip igmp snooping interface EXEC mode command displays the IGMP snooping configuration for a specific VLAN.

Syntax

show ip igmp snooping interface vlan-id

Parameters

interface vlan-id—Specifies the VLAN ID.

Command Mode

EXEC mode

Example

The following example displays the IGMP snooping configuration for VLAN 1000

switchxxxxxx# show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping admin: Enabled
IGMP Snooping oper: Enabled
Routers IGMP version: 3
Groups that are in IGMP version 2 compatibility mode:
231.2.2.3, 231.2.2.3
Groups that are in IGMP version 1 compatibility mode:
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3
IGMP snooping robustness: admin 2  oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
IGMP snooping query maximum response: admin 10 sec oper 10 sec
IGMP snooping last member query counter: admin 2 oper 2
IGMP snooping last member query interval: admin 1000 msec oper 500 msec
IGMP snooping last immediate leave: enable
Automatic learning of Multicast router ports is enabled

38.20 show ip igmp snooping groups

The show ip igmp snooping groups EXEC mode command displays the Multicast groups learned by the IGMP snooping.

Syntax

show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address] [source ip-address]

Parameters

vlan vlan-id—Specifies the VLAN ID.
address ip-multicast-address—Specifies the IP multicast address.
source ip-address—Specifies the IP source address.

Command Mode

EXEC mode

User Guidelines

To see all Multicast groups learned by IGMP snooping, use the show ip igmp snooping groups command without parameters.

Use the show ip igmp snooping groups command with parameters to see a needed subset of all Multicast groups learned by IGMP snooping

To see the full Multicast address table (including static addresses), use the show bridge multicast address-table command.
Example

The following example shows sample output for IGMP version 2.

```
switchxxxxxx# show ip igmp snooping groups
Vlan Group Address Source Address Include Ports Exclude Ports Comp-Mode
---- ----------- ---------- ---------- ---------- ------------
1 239.255.255.250 * gi1 ---------------- v3
```

38.21 show ip igmp snooping multicast-tv

The `show ip igmp snooping multicast-tv` EXEC mode command displays the IP addresses associated with Multicast TV VLANs.

Syntax

```
show ip igmp snooping multicast-tv [vlan vlan-id]
```

Parameters

vlan vlan-id—Specifies the VLAN ID.

Command Mode

EXEC mode

Example

The following example displays the IP addresses associated with all Multicast TV VLANs.

```
switchxxxxxx# show ip igmp snooping multicast-tv
VLAN IP Address
----- ----------
1000 239.255.0.0
1000 239.255.0.1
1000 239.255.0.2
1000 239.255.0.3
1000 239.255.0.4
```
38.22 show ip igmp snooping cpe vlans

The `show ip igmp snooping cpe vlans` EXEC mode command displays the CPE VLAN to Multicast TV VLAN mappings.

**Syntax**

```
show ip igmp snooping cpe vlans [vlan vlan-id]
```

**Parameters**

`vlan vlan-id` — Specifies the CPE VLAN ID.

**Command Mode**

EXEC mode

**Example**

The following example displays the CPE VLAN to Multicast TV VLAN mappings.

```
switchxxxxxx# show ip igmp snooping cpe vlans
CPE VLAN  Multicast-TV VLAN
---------  -------------------
  2         1118
  3         1119
```
IPv6 MLD Snooping Commands

### 39.1 ipv6 mld snooping (Global)

The `ipv6 mld snooping` Global Configuration mode command enables IPv6 Multicast Listener Discovery (MLD) snooping. To disable IPv6 MLD snooping, use the `no` form of this command.

**Syntax**

```
ipv6 mld snooping
no ipv6 mld snooping
```

**Parameters**

N/A

**Default Configuration**

IPv6 MLD snooping is disabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables IPv6 MLD snooping.

```
switchxxxxxx(config)# ipv6 mld snooping
```

### 39.2 ipv6 mld snooping vlan

Use the `ipv6 mld snooping vlan` Global Configuration mode command to enable MLD snooping on a specific VLAN. Use the `no` form of this command to disable MLD snooping on a VLAN interface.

**Syntax**

```
ipv6 mld snooping vlan vlan-id
```

---

---
no ipv6 mld snooping vlan vlan-id

Parameters

vlan-id—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

MLD snooping can only be enabled on static VLANs.

MLDv1 and MLDv2 are supported.

To activate MLD snooping, the Bridge Multicast Filtering command must be enabled.

The user guidelines of the bridge multicast ipv6 mode Interface VLAN Configuration command describe the configuration that can be written into the FDB as a function of the FDB mode, and the MLD version that is used in the network.

Example

switchxxxxxx(config)# ipv6 mld snooping vlan 2

39.3 ipv6 mld robustness

Use the ipv6 mld robustness interface Configuration mode command to change a value of MLD robustness. Use the no format of the command to return to default.

Syntax

ipv6 mld robustness count

no ipv6 mld robustness

Parameters

count - The number of expected packet losses on a link. (Range: 1–7)
Default Configuration
2

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld robustness 3

39.4 ipv6 mld snooping vlan mrouter
Use the ipv6 mld snooping vlan mrouter Global Configuration mode command to enable automatic learning of Multicast router ports. Use the no form of this command to remove the configuration.

Syntax
ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp
no ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp

Parameters
- vlan-id—Specifies the VLAN.
- pim-dvmrp—Learn Multicast router port by PIM, DVMRP and MLD messages.

Default Configuration
Learning pim-dvmrp is enabled.

Command Mode
Global Configuration mode
User Guidelines

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

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

### 39.5 `ipv6 mld snooping vlan mrouter`

Use the `ipv6 mld snooping vlan mrouter` Interface Configuration mode command to define a port that is connected to a Multicast router port. Use the `no` form of this command to remove the configuration.

Syntax

```
ipv6 mld snooping vlan vlan-id mrouter interface interface-list
no ipv6 mld snooping vlan vlan-id mrouter interface interface-list
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies a list of interfaces. The interfaces can be from one of the following types: port or port-channel.

Default Configuration

No ports defined

Command Mode

Interface Configuration mode

User Guidelines

This command may be used in conjunction with the `bridge multicast forward-all` command, which is used in older versions to statically configure a port as a Multicast router.

A port that is defined as a Multicast router port receives all MLD packets (reports and queries) as well as all Multicast data.
You can execute the command before the VLAN is created and for a range of ports as shown in the example.

**Example**

```
switchxxxxxx(config)interface gi1/1/1
switchxxxxxx(config-if)# ipv6 mld snooping vlan 1 mrouter interface gi1/1/1 - 10
```

### 39.6 ipv6 mld snooping vlan forbidden mrouter

Use the `ipv6 mld snooping vlan forbidden mrouter` Global Configuration mode command to forbid a port from being defined as a Multicast router port by static configuration or by automatic learning. Use the `no` form of this command to remove the configuration.

**Syntax**

```
ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list
no ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list
```

**Parameters**

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

**Default Configuration**

No forbidden ports by default

**Command Mode**

Global Configuration mode

**User Guidelines**

A port that is forbidden to be defined as a Multicast router port (mrouter port) cannot be learned dynamically or assigned statically.

The `bridge multicast forward-all` command was used in older versions to forbid dynamic learning of Multicast router ports.
You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface gi1
```

### 39.7 ipv6 mld snooping vlan static

Use the `ipv6 mld snooping vlan static` Global Configuration mode command to register an IPv6-layer Multicast address to the bridge table, and to add statically ports to the group. Use the `no` form of this command to remove ports specified as members of a static Multicast group.

#### Syntax

```
ipv6 mld snooping vlan vlan-id static ipv6-address interface [interface-list]
no ipv6 mld snooping vlan vlan-id static ipv6-address interface [interface-list]
```

#### Parameters

- `vlan-id`—Specifies the VLAN.
- `ipv6-address`—Specifies the IP multicast address
- `interface-list`—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

#### Default Configuration

No Multicast addresses are defined.

#### Command Mode

Global configuration mode

#### User Guidelines

Static multicast addresses can only be defined on static VLANs.

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 static 239.2.2.2 gi1

39.8 ipv6 mld query-interval

Use the ipv6 mld query-interval Interface Configuration mode command to configure the Query interval. Use the no format of the command to return to default.

Syntax

ipv6 mld query-interval seconds
ipv6 mld query-interval

Parameters

seconds—Frequency, in seconds, at which MLD query messages are sent on the interface. (Range: 30–18000)

Default Configuration

125

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides the frequency value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld query-interval 3000
39.9 ipv6 mld query-max-response-time

Use the `ipv6 mld query-max-response-time` Interface Configuration mode command to configure the Query Maximum Response time. Use the `no` format of the command to return to default.

Syntax

```
ipv6 mld query-max-response-time seconds
no ipv6 mld query-max-response-time
```

Parameter

`seconds`—Maximum response time, in seconds, advertised in MLD queries. (Range: 5–20)

Default Configuration

10

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides the maximum response time value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

```
switchxxxxx(config)# interface vlan 1
switchxxxxx(config-if)# ipv6 mld query-max-response-time 5
```

39.10 ipv6 mld last-member-query-count

Use the `ipv6 mld last-member-query-count` Interface Configuration mode command to configure the Last Member Query Count. This is the number of Multicast address specific queries sent before the router assumes there are no local listeners. The Last Listener Query Count is also the number of Multicast
Address and Source Specific Queries sent before the router assumes there are no listeners for a particular source.

Use the no format of the command to return to default.

Syntax

ipv6 mld last-member-query-count count
no ipv6 mld last-member-query-count

Parameters

count—The number of times that group- or group-source-specific queries are sent upon receipt of a Leave message. (Range: 1–7)

Default Configuration

The value of the Robustness variable.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides the maximum response time value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld last-member-query-count 3

39.11 ipv6 mld last-member-query-interval

Use the ipv6 mld last-member-query-interval interface configuration command to configure the Last Member Query Interval. Use the no format of the command to return to default.

Syntax

ipv6 mld last-member-query-interval milliseconds
no ipv6 mld last-member-query-interval

Parameter

milliseconds—Interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. (Range: 100–64512).

Default Configuration

1000

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides this value if it is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld last-member-query-interval 2000

39.12 ipv6 mld snooping vlan immediate-leave

Use the ipv6 mld snooping vlan immediate-leave Global Configuration mode command to enable MLD Snooping Immediate-Leave processing on a VLAN. When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD queries from the Multicast router, it deletes entries periodically if it does not receive any MLD membership reports from the Multicast clients.

MLD snooping Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface.

Use the no format of the command to return to disable MLD Snooping Immediate-Leave processing.
Syntax
ipv6 mld snooping vlan vlan-id immediate-leave
no ipv6 mld snooping vlan vlan-id immediate-leave

Parameters
vlan-id—Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
You can execute the command before the VLAN is created.

Example

switchxxxxxx(config)# ipv6 mld snooping vlan 1 immediate-leave

39.13 show ipv6 mld snooping mrouter

The show ipv6 mld snooping mrouter EXEC mode command displays information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN.

Syntax
show ipv6 mld snooping mrouter [interface vlan-id]

Parameters
interface vlan-id—Specifies the VLAN ID.

Default Configuration
Display information for all VLANs.
**Command Mode**

EXEC mode

**Example**

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000

```
switchxxxxxx# show ipv6 mld snooping mrouter interface 1000
VLAN  Static  Dynamic  Forbidden
   ----  ------  --------  --------
1000    gi1    gi2      gi3-23
```

**39.14 show ipv6 mld snooping interface**

The `show ipv6 mld snooping interface` EXEC mode command displays the IPv6 MLD snooping configuration for a specific VLAN.

**Syntax**

```
show ipv6 mld snooping interface vlan-id
```

**Parameters**

- **vlan-id**—Specifies the VLAN ID.

**Default Configuration**

Display information for all VLANs.

**Command Mode**

EXEC mode

**Example**

The following example displays the MLD snooping configuration for VLAN 1000.

```
switchxxxxxx# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
```
MLD Snooping admin: Enabled
MLD snooping oper mode: Enabled
Routers MLD version: 2
Groups that are in MLD version 1 compatibility mode:
FF12::3, FF12::8
MLD snooping robustness: admin 2  oper 2
MLD snooping query interval: admin 125 sec  oper 125 sec
MLD snooping query maximum 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 msec  oper 600 msec
MLD snooping last immediate leave: enable
Automatic learning of multicast router ports is enabled

39.15 show ipv6 mld snooping groups

The show ipv6 mld snooping groups EXEC mode command displays the multicast groups learned by the MLD snooping.

Syntax

show ipv6 mld snooping groups [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-address]

Parameters

- vlan vlan-id—Specifies the VLAN ID.
- address ipv6-multicast-address—Specifies the IPv6 multicast address.
- source ipv6-address—Specifies the IPv6 source address.

Command Mode

EXEC mode

Default Configuration

Display information for all VLANs and addresses defined on them.
User Guidelines

To see the full multicast address table (including static addresses), use the `show bridge multicast address-table` command.

The Include list contains the ports which are in a forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports which have issued an explicit Exclude for that specific source in a multicast group.

The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in a multicast bridge.

Note: Under certain circumstances, the Exclude list may not contain accurate information; for example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list.

Example

The following example shows the output for show ipv6 mld snooping groups.

```
switchxxxxxx# show ipv6 mld snooping groups

VLAN  Group Address  Source Address  Include Ports  Exclude Ports
       -------------------  -------------------  -----------  ------------
1      FF12::3        FE80::201:C9FF:FE40:8001  gi1         gi2
1      FF12::3        FE80::201:C9FF:FE40:8002  gi2
19     FF12::8        FE80::201:C9FF:FE40:8003  gi9
19     FF12::8        FE80::201:C9FF:FE40:8004  gi1  gi2  2
19     FF12::8        FE80::201:C9FF:FE40:8005  gi10-11  gi3  2

MLD Reporters that are forbidden statically:
VLAN  Group Address  Source Address  Ports
      -------------------  -------------------  ---------
1      FF12::3        FE80::201:C9FF:FE40:8001  gi8
19     FF12::8        FE80::201:C9FF:FE40:8001  gi9
```
Link Aggregation Control Protocol (LACP) Commands

40.1 lACP system-priority

Use the lACP system-priority Global Configuration mode command to set the system priority. Use the no form of this command to restore the default configuration.

Syntax

lACP system-priority value

no lACP system-priority

Parameters

value—Specifies the system priority value. (Range: 1–65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

Example

The following example sets the system priority to 120.

switchxxxxxx(config)# lACP system-priority 120

40.2 lACP port-priority

Use the lACP port-priority Interface Configuration (Ethernet) mode command to set the physical port priority. Use the no form of this command to restore the default configuration.

Syntax

lACP port-priority value
no lacp port-priority

Parameters

value—Specifies the port priority. (Range: 1 use the no form of this command 65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example sets the priority of gi6.

```plaintext
switchxxxxx(config)# interface gi6
switchxxxxx(config-if)# lacp port-priority 247
```

### 40.3  lacp timeout

Use the lacp timeout Interface Configuration (Ethernet) mode command to assign an administrative LACP timeout to an interface. Use the no form of this command to restore the default configuration.

Syntax

lacp timeout \{long \| short\}

no lacp timeout

Parameters

- long—Specifies the long timeout value.
- short—Specifies the short timeout value.

Default Configuration

The default port timeout value is Long.
Command Mode

Interface Configuration (Ethernet) mode

Example

The following example assigns a long administrative LACP timeout to gi6.

```
switchxxxxx(config)# interface gi6
switchxxxxx(config-if)# lACP timeout long
```

40.4 show lACP

Use the show lACP EXEC mode command to display LACP information for all Ethernet ports or for a specific Ethernet port.

Syntax

```
show lACP interface-id [parameters | statistics | protocol-state]
```

Parameters

- **interface-id** — Specify an interface ID. The interface ID must be an Ethernet port
- **parameters** — Displays parameters only.
- **statistics** — Displays statistics only.
- **protocol-state** — Displays protocol state only.

Command Mode

EXEC mode

Example

The following example displays LACP information for gi1.

```
switchxxxxx# show lACP ethernet gi1
Port gi1 LACP parameters:
  Actor
```
system priority: 1
system mac addr: 00:00:12:34:56:78
port Admin key: 30
port Oper key: 30
port Oper number: 21
port Admin priority: 1
port Oper priority: 1
port Admin timeout: LONG
port Oper timeout: LONG
LACP Activity: ACTIVE
Aggregation: AGGREGATABLE
synchronization: FALSE
collecting: FALSE
distributing: FALSE
expired: FALSE

Partner
system priority: 0
system mac addr: 00:00:00:00:00:00
port Admin key: 0
port Oper key: 0
port Oper number: 0
port Admin priority: 0
port Oper priority: 0
port Admin timeout: LONG
port Oper timeout: LONG
LACP Activity: PASSIVE
Aggregation: AGGREGATABLE
synchronization: FALSE
collecting: FALSE
distributing: FALSE
expired: FALSE

Port gi1 LACP Statistics:
LACP PDUs sent: 2
LACP PDUs received: 2
Port gi1 LACP Protocol State:
LACP State Machines:
  Receive FSM: Port Disabled State
  Mux FSM: Detached State
40.5  show lacp port-channel

Use the **show lacp port-channel** EXEC mode command to display LACP information for a port-channel.

**Syntax**

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

**Parameters**

- **port_channel_number**—Specifies the port-channel number.

**Command Mode**

EXEC mode

**Example**

The following example displays LACP information about port-channel 1.

```
switchxxxxxx# show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet
   Actor
```
System  
Priority: 1  
MAC Address: 000285:0E1C00  
Admin Key: 29  
Oper Key: 29

Partner  
System 0  
Priority: 00:00:00:00:00:00  
MAC Address: 14  
Oper Key:
GARP VLAN Registration Protocol (GVRP) Commands

41.1  gvrp enable (Global)

Use the `gvrp enable` Global Configuration mode command to enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally. Use the `no` form of this command to disable GVRP on the device.

Syntax

```
gvrp enable
no gvrp enable
```

Parameters

N/A

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

The following example enables GVRP globally on the device.

```
switchxxxxxx(config)# gvrp enable
```

41.2  gvrp enable (Interface)

Use the `gvrp enable` Interface Configuration (Ethernet, Port-channel) mode command to enable GVRP on an interface. Use the `no` form of this command to disable GVRP on an interface.

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 only. 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
The following example enables GVRP on gi6.

```
switchxxxxxx(config)# interface gi6
switchxxxxxx(config-if)# gvrp enable
```

41.3 gvrp vlan-creation-forbid

Use the `gvrp vlan-creation-forbid` Interface Configuration mode command to disable dynamic VLAN creation or modification. Use the `no` form of this command to enable dynamic VLAN creation or modification.

Syntax

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

Default Configuration
Enabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode
Example

The following example disables dynamic VLAN creation on gi3.

switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# gvrp vlan-creation-forbid

41.4 gvrp registration-forbid

Use the `gvrp registration-forbid` Interface Configuration mode command to deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port. Use the `no` form of this command to allow dynamic registration of VLANs on a port.

Syntax

`gvrp registration-forbid`

`no gvrp registration-forbid`

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example forbids dynamic registration of VLANs on gi2.

switchxxxxxx(config)# interface gi2
switchxxxxxx(config-if)# gvrp registration-forbid

41.5 clear gvrp statistics

Use the `clear gvrp statistics` Privileged EXEC mode command to clear GVRP statistical information for all interfaces or for a specific interface.
**Syntax**

```
clear gvrp statistics [interface-id]
```

**Parameters**

- **Interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Default Configuration**

All GVRP statistics are cleared.

**Command Mode**

Privileged EXEC mode

**Example**

The following example clears all GVRP statistical information on gi5.

```
switchxxxxxx# clear gvrp statistics gi5
```

### 41.6 *show gvrp configuration*

Use the `show gvrp configuration` EXEC mode command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP.

**Syntax**

```
show gvrp configuration [interface-id | detailed]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

- **detailed**—Displays information for non-present ports in addition to present ports.

**Default Configuration**

All GVRP statistics are displayed for all interfaces. If detailed is not used, only present ports are displayed.
Command Mode
EXEC mode

Example
The following example displays GVRP configuration.

```
switchxxxxxx# show gvrp configuration
GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094
Port(s) GVRP-Status Regist-      Dynamic            Timers(ms)
        ration VLAN Creation    Join  Leave  Leave All
    ----  ----------- --------    -------------    ----    -----   ----------
gi1    Enabled     Forbidden   Disabled         600     200    10000
gi2    Enabled     Normal      Enabled          1200    400    20000
```

41.7 show gvrp statistics
Use the `show gvrp statistics` EXEC mode command to display GVRP statistics for all interfaces or for a specific interface.

Syntax
```
show gvrp statistics [interface-id]
```

Parameters
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
All GVRP statistics are displayed.

Command Mode
EXEC mode
Example

The following example displays GVRP statistical information.

```
switchxxxxxx# show gvrp statistics
```

GVRP statistics:

Legend:

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

<table>
<thead>
<tr>
<th>Port</th>
<th>rJE</th>
<th>rJIn</th>
<th>rEmp</th>
<th>rLIn</th>
<th>rLE</th>
<th>rLA</th>
<th>sJE</th>
<th>sJIn</th>
<th>sEmp</th>
<th>sLIn</th>
<th>sLE</th>
<th>sLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gi8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

41.8 show gvrp error-statistics

Use the `show gvrp error-statistics` EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

Syntax

```
show gvrp error-statistics [interface-id]
```

Parameters

- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
Default Configuration
All GVRP error statistics are displayed.

Command Mode
EXEC mode

Example
The following example displays GVRP error statistics.

```plaintext
switchxxxxxx# show gvrp error-statistics
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 INVAVAL INVALEN 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
```
42.1  ip dhcp snooping

Use the ip dhcp snooping Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the no form of this command to restore the default configuration.

Syntax
ip dhcp snooping
no ip dhcp snooping

Parameters
N/A

Default Configuration
DHCP snooping is disabled.

Command Mode
Global Configuration mode

User Guidelines
For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the ip dhcp snooping vlan Global Configuration mode command.

Example
The following example enables DHCP Snooping on the device.

```
switchxxxxxxx(config)# ip dhcp snooping
```
42.2 ip dhcp snooping vlan

Use the ip dhcp snooping vlan Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the no form of this command to disable DHCP Snooping on a VLAN.

Syntax

```
ip dhcp snooping vlan vlan-id
no ip dhcp snooping vlan-id
```

Parameters

- **vlan-id**: Specifies the VLAN ID.

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example

The following example enables DHCP Snooping on VLAN 21.

```
switchxxxxxx(config)# ip dhcp snooping vlan 21
```

42.3 ip dhcp snooping trust

Use the ip dhcp snooping trust Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to restore the default configuration.

Syntax

```
ip dhcp snooping trust
```

no ip dhcp snooping trust

Parameters
N/A

Default Configuration
The interface is untrusted.

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

User Guidelines
Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example
The following example configures gi5 as trusted for DHCP Snooping.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# ip dhcp snooping trust
```

### 42.4 ip dhcp snooping information option allowed-untrusted

Use the `ip dhcp snooping information option allowed-untrusted` Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the `no` form of this command to drop these packets from an untrusted port.

Syntax

```
ip dhcp snooping information option allowed-untrusted
```

Parameters
N/A
Default Configuration
DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode
Global Configuration mode

Example
The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
switchxxxxxx(config)# ip dhcp snooping information option allowed-untrusted
```

42.5  ip dhcp snooping verify
Use the ip dhcp snooping verify Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the no form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

Syntax
```
ip dhcp snooping verify
no ip dhcp snooping verify
```

Default Configuration
The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

Command Mode
Global Configuration mode

Example
The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
switchxxxxxx(config)# ip dhcp snooping verify
```
42.6 ip dhcp snooping database

Use the `ip dhcp snooping database` Global Configuration mode command to enable the DHCP Snooping binding database file. Use the `no` form of this command to delete the DHCP Snooping binding database file.

Syntax

```
ip dhcp snooping database
no ip dhcp snooping database
```

Parameters

N/A

Default Configuration

The DHCP Snooping binding database file is not defined.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example

The following example enables the DHCP Snooping binding database file.

```
switchxxxxxx(config)# ip dhcp snooping database
```

42.7 ip dhcp snooping database update-freq

Use the `ip dhcp snooping database update-freq` Global Configuration mode command to set the update frequency of the DHCP Snooping binding database file. Use the `no` form of this command to restore the default configuration.
DHCP Snooping and ARP Inspection Commands

42

Syntax
ip dhcp snooping database update-freq seconds
no ip dhcp snooping database update-freq

Parameters
seconds—Specifies the update frequency in seconds. (Range: 600–86400)

Default Configuration
The default update frequency value is 1200 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the DHCP Snooping binding database file update frequency to 1 hour.

switchxxxxxx(config)# ip dhcp snooping database update-freq 3600

42.8 ip dhcp snooping binding

Use the ip dhcp snooping binding Privileged EXEC mode command to configure the DHCP Snooping binding database and add binding entries to the database. Use the no form of this command to delete entries from the binding database.

Syntax
ip dhcp snooping binding mac-address vlan-id ip-address interface-id expiry {seconds | infinite}
no ip dhcp snooping binding mac-address vlan-id

Parameters
- mac-address—Specifies a MAC address.
- vlan-id—Specifies a VLAN number.
- ip-address—Specifies an IP address.
DHCP Snooping and ARP Inspection Commands

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
  - **expiry**
  -  **seconds**—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967295)
  -  **infinite**—Specifies infinite lease time.

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry is displayed in the show commands as a DHCP Snooping entry.

The user cannot delete dynamic temporary entries for which the IP address is 0.0.0.0.

The user can add static entry to the DHCP Snooping database by using the command `ip source-guard binding`.

Example

The following example adds a binding entry to the DHCP Snooping binding database.

```
switchxxxxxx# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 gi5
expiry 900
```

42.9   **clear ip dhcp snooping database**

Use the `clear ip dhcp snooping database` Privileged EXEC mode command to clear the DHCP Snooping binding database.
**42 DHCP Snooping and ARP Inspection Commands**

### clear ip dhcp snooping database

**Syntax**

clear ip dhcp snooping database

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**Example**

The following example clears the DHCP Snooping binding database.

```
switchxxxxxx# clear ip dhcp snooping database
```

### 42.10 show ip dhcp snooping

Use the `show ip dhcp snooping` EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

**Syntax**

```
show ip dhcp snooping [interface-id]
```

**Parameters**

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode

**Example**

The following example displays the DHCP snooping configuration.

```
switchxxxxxx# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
```
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>Yes</td>
</tr>
<tr>
<td>gi2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 42.11 show ip dhcp snooping binding

Use the `show ip dhcp snooping binding` User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

**Syntax**

```
show ip dhcp snooping binding [mac-address mac-address] [ip-address ip-address] [vlan vlan-id] [interface-id]
```

**Parameters**

- **mac-address mac-address**—Specifies a MAC address.
- **ip-address ip-address**—Specifies an IP address.
- **vlan vlan-id**—Specifies a VLAN ID.
- **interface-id**— Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

User EXEC mode
Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.

```
switchxxxxxx# show ip dhcp snooping binding
```

Update frequency: 1200
Total number of binding: 2

<table>
<thead>
<tr>
<th>Mac Address</th>
<th>IP Address</th>
<th>Lease (sec)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0060.704C.73FF</td>
<td>10.1.8.1</td>
<td>7983</td>
<td>snooping</td>
<td>3</td>
<td>gi21</td>
</tr>
<tr>
<td>0060.704C.7BC1</td>
<td>10.1.8.2</td>
<td>92332</td>
<td>snooping</td>
<td>3</td>
<td>gi22</td>
</tr>
</tbody>
</table>

### 42.12 ip source-guard

Use the `ip source-guard` command in Configuration or Interface mode to enable IP Source Guard globally on a device or in Interface Configuration (Ethernet, Port-channel) mode to enable IP Source Guard on an interface.

Use the `no` form of this command to disable IP Source Guard on the device or on an interface.

**Syntax**

```plaintext
ip source-guard
no ip source-guard
```

**Parameters**

N/A

**Default Configuration**

IP source guard is disabled.

**Command Mode**

Configuration or Interface Configuration (Ethernet, Port-channel) mode
User Guidelines

IP Source Guard must be enabled globally before enabling IP Source Guard on an interface.

IP Source Guard is active only on DHCP snooping untrusted interfaces, and if at least one of the interface VLANs are DHCP snooping enabled.

Example

The following example enables IP Source Guard on gi5.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# ip source-guard
```

42.13 ip source-guard binding

Use the `ip source-guard binding` Global Configuration mode command to configure the static IP source bindings on the device. Use the `no` form of this command to delete the static bindings.

Syntax

```
ip source-guard binding mac-address vlan-id ip-address {interface-id}
no ip source-guard binding mac-address vlan-id
```

Parameters

- `mac-address`—Specifies a MAC address.
- `vlan-id`—Specifies a VLAN number.
- `ip-address`—Specifies an IP address.
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No static binding exists.

Command Mode

Global Configuration mode
User Guidelines

The device currently supports filtering that is based only on the source IP address. In future, the device might support filtering mode that is based on the MAC address and IP source address. Currently the MAC address field is an informative field.

Example

The following example configures the static IP source bindings.

```
switchxxxxxx(config)# ip source-guard binding 0060.704C.73FF 23 176.10.1.1 gi5
```

42.14 ip source-guard tcam retries-freq

Use the `ip source-guard tcam retries-freq` Global Configuration mode command to set the frequency of retries for TCAM resources for inactive IP Source Guard addresses. Use the `no` form of this command to restore the default configuration.

Syntax

```
ip source-guard tcam retries-freq {seconds / never}
no ip source-guard tcam retries-freq
```

Parameters

- `seconds`—Specifies the retries frequency in seconds. (Range: 10–600)
- `never`—Disables automatic searching for TCAM resources.

Default Configuration

The default retries frequency is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.
By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses. Use this command to change the search frequency or to disable automatic retries for TCAM space.

The `ip source-guard tcam locate` Privileged EXEC mode command manually retries locating TCAM resources for the inactive IP Source Guard addresses.

The `show ip source-guard inactive` EXEC mode command displays the inactive IP Source Guard addresses.

**Example**

The following example sets the frequency of retries for TCAM resources to 2 minutes.

```
switchxxxxxxx(config)# ip source-guard tcam retries-freq 120
```

### 42.15 ip source-guard tcam locate

Use the `ip source-guard tcam locate` Privileged EXEC mode command to manually retry to locate TCAM resources for inactive IP Source Guard addresses.

**Syntax**

```
ip source-guard tcam locate
```

**Parameters**

N/A

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Execute the `ip source-guard tcam retries-freq never` Global Configuration mode command to disable automatic retries for TCAM space, and then execute this
command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

The `show ip source-guard inactive` EXEC mode command displays the inactive IP source guard addresses.

**Example**

The following example manually retries to locate TCAM resources.

```
switchxxxxxx# ip source-guard tcam locate
```

### 42.16 `show ip source-guard configuration`

Use the `show ip source-guard configuration` EXEC mode command to display the IP source guard configuration for all interfaces or for a specific interface.

**Syntax**

```
show ip source-guard configuration [interface-id]
```

**Parameters**

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode
Example

The following example displays the IP Source Guard configuration.

```
switchxxxxxx# show ip source-guard configuration
IP source guard is globally enabled.
Interface State
--------- -------
gi21 Enabled
 gi22 Enabled
 gi23 Enabled
 gi24 Enabled
 gi32 Enabled
 gi33 Enabled
 gi34 Enabled
```

42.17 show ip source-guard status

Use the **show ip source-guard status** EXEC mode command to display the IP Source Guard status.

**Syntax**

```
show ip source-guard status [mac-address mac-address] [ip-address ip-address]
[vlan vlan] [interface-id]
```

**Parameters**

- **mac-address mac-address**—Specifies a MAC address.
- **ip-address ip-address**—Specifies an IP address.
- **vlan vlan-id**—Specifies a VLAN ID.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode
Example

The following examples display the IP Source Guard status.

```
switchxxxxxx# show ip source-guard status
IP source guard is globally disabled.
switchxxxxxx# show ip source-guard status

+-------------+----------+---------+----------+----------+-------+-------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter</th>
<th>Status</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi21</td>
<td>IP</td>
<td>Active</td>
<td>10.1.8.1</td>
<td>0060.704c.73ff</td>
<td>3</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi22</td>
<td>IP</td>
<td>Active</td>
<td>10.1.8.2</td>
<td>0060.704c.7bc1</td>
<td>3</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi23</td>
<td>IP</td>
<td>Active</td>
<td>10.1.12.2</td>
<td>0060.704c.7bc3</td>
<td>4</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi24</td>
<td>IP</td>
<td>Active</td>
<td>Deny all</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi25</td>
<td>IP</td>
<td>Active</td>
<td>10.1.8.218</td>
<td>0060.704c.7bac</td>
<td>3</td>
<td>Static</td>
</tr>
<tr>
<td>gi32</td>
<td>IP</td>
<td>Inactive</td>
<td>10.1.8.32</td>
<td>0060.704c.83ff</td>
<td>3</td>
<td>DHCP</td>
</tr>
<tr>
<td>gi33</td>
<td>IP</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi34</td>
<td>IP</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gi35</td>
<td>IP</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
+-------------+----------+---------+------------+-------------+-------+-------+
```

42.18 show ip source-guard inactive

Use the `show ip source-guard inactive` EXEC mode command to display the IP Source Guard inactive addresses.

Syntax

```
show ip source-guard inactive
```

Parameters

N/A

Command Mode

EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.
Use the `ip source-guard tcam retries-freq` Global Configuration mode command to change the retry frequency or to disable automatic retries for TCAM space.

Use the `ip source-guard tcam locate` Privileged EXEC mode command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

This command displays the inactive IP source guard addresses.

**Example**

The following example displays the IP source guard inactive addresses.

```
switchxxxxxx# show ip source-guard inactive
```

TBD: TCAM resources search frequency: 10 minutes

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>Type</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi32</td>
<td>IP</td>
<td>10.1.8.32</td>
<td>0060.704C.8</td>
<td>3</td>
<td>DHCP</td>
<td>Resource Problem</td>
</tr>
<tr>
<td>gi33</td>
<td>IP</td>
<td>10.1.8.32</td>
<td>3FF</td>
<td></td>
<td></td>
<td>Trust port</td>
</tr>
<tr>
<td>gi34</td>
<td>I</td>
<td>10.1.8.32</td>
<td></td>
<td></td>
<td></td>
<td>No snooping VLAN</td>
</tr>
</tbody>
</table>

### 42.19 show ip source-guard statistics

Use the `show ip source-guard statistics` EXEC mode command to display the Source Guard dynamic information (permitted stations).

**Syntax**

```
show ip source-guard statistics [vlan vlan-id]
```

**Parameters**

`vlan-id`—Display the statistics on this VLAN.

**Command Mode**

EXEC mode

**Example**

```
switchxxxxxx# show ip source-guard statistics
```
42.20  ip arp inspection

Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

**Syntax**

```plaintext
ip arp inspection

no ip arp inspection
```

**Parameters**

N/A

**Default Configuration**

ARP inspection is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

**Example**

The following example enables ARP inspection on the device.

```
switchxxxxxx(config)# ip arp inspection
```
42.21 ip arp inspection vlan

Use the `ip arp inspection vlan` Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the `no` form of this command to disable ARP inspection on a VLAN.

**Syntax**

```
ip arp inspection vlan vlan-id
no ip arp inspection vlan vlan-id
```

**Parameters**

- `vlan-id`—Specifies the VLAN ID.

**Default Configuration**

DHCP Snooping based ARP inspection on a VLAN is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the `ip arp inspection list assign` Global Configuration mode command to enable static ARP inspection.

**Example**

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
switchxxxxxx(config)# ip arp inspection vlan 23
```

---

**42.22 ip arp inspection trust**

Use the `ip arp inspection trust` Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the `no` form of this command to restore the default configuration.
Syntax

ip arp inspection trust
no ip arp inspection trust

Parameters

N/A

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device 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. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the ip arp inspection log-buffer vlan Global Configuration mode command.

Example

The following example configures gi3 as a trusted interface.

```bash
switchxxxxxx(config)# interface gi3
switchxxxxxx(config-if)# ip arp inspection trust
```

42.23  ip arp inspection validate

Use the ip arp inspection validate Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the no form of this command to restore the default configuration.
Syntax

ip arp inspection validate
no ip arp inspection validate

Parameters

N/A

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address**: Compares the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.

- **Destination MAC address**: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.

- **IP addresses**: 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.

Example

The following example executes ARP inspection validation.

```
switchxxxxxx(config)# ip arp inspection validate
```

42.24  ip arp inspection list create

Use the **ip arp inspection list create** Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the **no** form of this command to delete the list.
DHCP Snooping and ARP Inspection Commands

### ip arp inspection list create name

**Syntax**

```
ip arp inspection list create name
```

**Parameters**

- `name`—Specifies the static ARP binding list name. (Length: 1–32 characters)

**Default Configuration**

No static ARP binding list exists.

**Command Mode**

Global Configuration mode

**User Guidelines**

Use the `ip arp inspection list assign` command to assign the list to a VLAN.

**Example**

The following example creates the static ARP binding list ‘servers’ and enters the ARP list configuration mode.

```
switchxxxxxx(config)# ip arp inspection list create servers
switchxxxxxx(config-ARP-list)#
```

### ip mac

Use the `ip mac` ARP-list Configuration mode command to create a static ARP binding. Use the `no` form of this command to delete a static ARP binding.

**Syntax**

```
ip ip-address mac mac-address
no ip ip-address mac mac-address
```

**Parameters**

- `ip-address`—Specifies the IP address to be entered to the list.
- `mac-address`—Specifies the MAC address associated with the IP address.
Default Configuration
No static ARP binding is defined.

Command Mode
ARP-list Configuration mode

Example
The following example creates a static ARP binding.

```
switchxxxxxx(config)# ip arp inspection list create servers
switchxxxxxx(config-ARP-list)# ip 172.16.1.1 mac 0060.704C.7321
switchxxxxxx(config-ARP-list)# ip 172.16.1.2 mac 0060.704C.7322
```

42.26  ip arp inspection list assign

Use the `ip arp inspection list assign` Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the `no` form of this command to delete the assignment.

Syntax
```
ip arp inspection list assign  vlan-id  name
no ip arp inspection list assign  vlan-id
```

Parameters
- `vlan-id`—Specifies the VLAN ID.
- `name`—Specifies the static ARP binding list name.

Default Configuration
No static ARP binding list assignment exists.

Command Mode
Global Configuration mode
Example
The following example assigns the static ARP binding list Servers to VLAN 37.

```
switchxxxxxx(config)# ip arp inspection list assign 37 servers
```

### 42.27 ip arp inspection logging interval

Use the `ip arp inspection logging interval` Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
ip arp inspection logging interval {seconds / infinite}
o no ip arp inspection logging interval
```

**Parameters**

- `seconds`—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- `infinite`—Specifies that SYSLOG messages are not generated.

**Default Configuration**

The default minimum ARP SYSLOG message logging time interval is 5 seconds.

**Command Mode**

Global Configuration mode

**Example**

The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
switchxxxxxx(config)# ip arp inspection logging interval 60
```
42.28  show ip arp inspection

Use the `show ip arp inspection` EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

**Syntax**

`show ip arp inspection [interface-id]`

**Parameters**

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**Command Mode**

EXEC mode

**Example**

The following example displays the ARP inspection configuration.

```
switchxxxxxx# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222 seconds

Interface    Trusted
------------ -----------
gi1          Yes

```

42.29  show ip arp inspection list

Use the `show ip arp inspection list` Privileged EXEC mode command to display the static ARP binding list.

**Syntax**

`show ip arp inspection list`
DHCP Snooping and ARP Inspection Commands

Parameters
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the static ARP binding list.

```
switchxxxxxx# show ip arp inspection list
List name: servers
Assigned to VLANs: 1,2
IP                ARP
172.16.1.1        0060.704C.7322
172.16.1.2        0060.704C.7322
```

42.30  show ip arp inspection statistics

Use the `show ip arp inspection statistics` EXEC command to display Statistics For The Following Types Of Packets That Have Been Processed By This Feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax

```
show ip arp inspection statistics [vlan vlan-id]
```

Parameters

- `vlan-id`—Specifies VLAN ID.

Command Mode
EXEC mode

User Guidelines

To clear ARP Inspection counters use the `clear ip arp inspection statistics` CLI command. Counters values are kept when disabling the ARP Inspection feature.
### Example

```
switchxxxxxx# show ip arp inspection statistics
Vlan  Forwarded Packets  Dropped Packets  IP/MAC Failures
----  ------------------  ------------------  ------------------
 2    1500100            80
```

### clear ip arp inspection statistics

Use the `clear ip arp inspection statistics` Privileged EXEC mode command to clear ARP Inspection statistics globally.

#### Syntax

```
clear ip arp inspection statistics [vlan vlan-id]
```

#### Parameters

- `vlan-id`—Specifies VLAN ID

#### Command Mode

Privileged EXEC mode

#### Example

```
switchxxxxxx# clear ip arp inspection statistics
```
IP Addressing Commands

43.1 ip address

Use the ip address Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the no form of this command to remove an IP address definition.

Syntax

If the product is in Layer 3 (Router mode).

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

If the product is in Layer 2 (Switch mode).

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

Parameters

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

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

Defining a static IP address on an interface implicitly removes the DHCP client configuration on the interface.
If the device is in Layer 3 router mode, it supports multiple IP addresses. The IP addresses must be from different IP subnets.

If the IP address is configured in Interface context, the IP address is bound to the interface in that context.

If a static IP address is already defined, the user must do no IP address in the relevant interface context before changing the IP address.

**Example**

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

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

### 43.2 ip address dhcp

Use the **ip address dhcp** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the no form of this command to release an acquired IP address.

**Syntax**

```
ip address dhcp
no ip address dhcp
```

**Parameters**

N/A

**Command Mode**

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

**User Guidelines**

This command enables any interface to dynamically learn its IP address by using the DHCP protocol.
DHCP client configuration on an interface implicitly removes the static IP address configuration on the interface.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

The `no ip address dhcp` command releases any IP address that was acquired, and sends a DHCPRELEASE message.

**Example**

The following example acquires an IP address for `gi16` from DHCP.

```
switchxxxxxx(config)# interface gi16
switchxxxxxx(config-if)# ip address dhcp
```

### 43 3 renew dhcp

Use the `renew dhcp` Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

**Syntax**

`renew dhcp [interface-id] [force-autoconfig]`

**Parameters**

- `interface-id`—Only required in routing mode (Layer 3). Specifies an interface ID (Ethernet port, Port-channel or VLAN).
- `force-autoconfig` - If the DHCP server holds a DHCP option 67 record for the assigned IP address, the record overwrites the existing device configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Note the following:
When the device is in Layer 2 (switch mode), interface-id is not required.

This command does not enable DHCP on an interface. If DHCP is not enabled on the requested interface, the command returns an error message.

If DHCP is enabled on the interface and an IP address was already acquired, the command tries to renew that IP address.

If DHCP is enabled on the interface and an IP address has not yet been acquired, the command initiates a DHCP request.

Example
The following example renews an IP address that was acquired from a DHCP server for VLAN 19. This assumes that the device is in Layer 3.

```
switchxxxxxx# renew dhcp vlan 19
```

43 4  ip default-gateway

The `ip default-gateway` Global Configuration mode command defines a default gateway (device). Use the `no` form of this command to restore the default configuration.

Syntax

```
ip default-gateway  ip-address
no  ip default-gateway
```

Parameters

`ip-address`—Specifies the default gateway IP address.

Command Mode

Global Configuration mode

Default Configuration

No default gateway is defined.
Example

The following example defines default gateway 192.168.1.1.

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

43 5  show ip interface

Use the `show ip interface` EXEC mode command to display the usability status of configured IP interfaces.

Syntax

```
show ip interface [interface-id]
```

Parameters

`interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration

All IP addresses.

Command Mode

EXEC mode

Examples

Example 1 - The following example displays the configured IP interfaces and their types when the device is in Router mode.

```
switchxxxxxx# show ip interface

+-------------+------+-+----------------+----------+--------+-
| IP Address  | I/F  | Type | Directed   | Precedence | Status |
|-------------|------|--|------------|------------|--------|--
| 10.5.234.232/24 | vlan 1 | Static | disable | No        | Valid  |
```


Example 2 - The following example displays the configured IP interfaces and their types when the device is in Switch mode.

```
switchxxxxxx# show ip interface
```

<table>
<thead>
<tr>
<th>Gateway IP Address</th>
<th>Activity status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.234.254</td>
<td>Active</td>
<td>static</td>
</tr>
</tbody>
</table>

```
switchxxxxxx# show ip interface
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>I/F</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.234.207/24</td>
<td>vlan 1</td>
<td>Static</td>
<td>Valid</td>
</tr>
</tbody>
</table>

**43 6  arp**

Use the `arp` Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the `no` form of this command to remove an entry from the ARP cache.

**Syntax**

```
arp ip-address mac-address [interface-id]
no arp ip-address
```

**Parameters**

- `ip-address`—IP address or IP alias to map to the specified MAC address.
- `mac-address`—MAC address to map to the specified IP address or IP alias.
- `interface-id`—Address pair is added for specified interface that can be Ethernet port, Port-channel or VLAN.

**Command Mode**

Global Configuration mode

**Default Configuration**

No permanent entry is defined.

If no interface ID is entered, address pair is relevant to all interfaces.
**User Guidelines**

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

**Example**

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
switchxxxxxx(config)# arp 198.133.219.232 00:00:0c:40:0f:bc gi6
```

### 43 7  **arp timeout (Global)**

Use the `arp timeout` Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
arp timeout seconds

no arp timeout
```

**Parameters**

- **seconds**—Specifies the time interval (in seconds) during which an entry remains in the ARP cache.
  
  (Range: 1–40000000)

**Default Configuration**

The default ARP timeout is 60000 seconds in Router mode, and 300 seconds in Switch mode.

**Command Mode**

Global Configuration mode

**Example**

The following example configures the ARP timeout to 12000 seconds.

```
switchxxxxxx(config)# arp timeout 12000
```
**43 8 ip arp proxy disable**

Use the `ip arp proxy disable` Global Configuration mode command to globally disable proxy Address Resolution Protocol (ARP). Use the `no` form of this command reenable proxy ARP.

This command can only be used when the device is in Router mode.

**Syntax**

```
ip arp proxy disable
no ip arp proxy disable
```

**Parameters**

N/A

**Default**

Disabled by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

This command overrides any proxy ARP interface configuration. To use this command, you must put the switch into routing mode using `set system`.

**Example**

The following example globally disables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config)# ip arp proxy disable
```

---

**43 9 ip proxy-arp**

Use the `ip proxy-arp` Interface Configuration mode command to enable an ARP proxy on specific interfaces. Use the `no` form of this command disable it.

This command can only be used when the device is in Router mode.
### Syntax

```plaintext
ip proxy-arp
no ip proxy-arp
```

### Default Configuration

ARP Proxy is enabled.

### Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

### User Guidelines

This configuration can be applied only if at least one IP address is defined on a specific interface. To use this command, you must put the switch into routing mode using `set system`.

### Example

The following example enables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config-if)# ip proxy-arp
```

### 43 10 clear arp-cache

Use the `clear arp-cache` Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

### Syntax

```plaintext
clear arp-cache
```

### Command Mode

Privileged EXEC mode

### Example

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

```
switchxxxxxx# clear arp-cache
```
43 11 show arp

Use the show arp Privileged EXEC mode command to display entries in the ARP table.

Syntax

`show arp [ip-address ip-address] [mac-address mac-address] [interface-id]`

Parameters

- `ip-address ip-address`—Specifies the IP address.
- `mac-address mac-address`—Specifies the MAC address.
- `interface-id`—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

User Guidelines

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

Example

The following example displays entries in the ARP table.

```
switchxxxxxx# show arp
ARP timeout: 80000 Seconds
VLAN Interface    IP Address    HW Address     Status
------- -------- ----------- ---------- -------
VLAN 1    gi1    10.7.1.102  00:10:B5:04:DB:4B Dynamic
VLAN 1    gi2    10.7.1.135  00:50:22:00:2A:A4 Static
```
### 43 12 show arp configuration

Use the `show arp configuration` privileged EXEC command to display the global and interface configuration of the ARP protocol.

**Syntax**

`show arp configuration`

**Parameters**

This command has no arguments or key words.

**Command Mode**

Privileged EXEC mode

**Example**

```
switchxxxxxx# show arp configuration
Global configuration:
    ARP Proxy: enabled
    ARP timeout:  80000 Seconds
Interface configuration:
    g2:
        ARP Proxy: disabled
        ARP timeout:60000 Seconds
    VLAN 1:
        ARP Proxy: enabled
        ARP timeout:70000 Seconds
    VLAN 2:
        ARP Proxy: enabled
        ARP timeout:80000 Second (Global)
```
### 43 13  interface ip

Use the `interface ip` Global Configuration mode command to enter the IP Interface Configuration mode.

This command can only be used when the device is in Router mode.

**Syntax**

```plaintext
interface ip-address
```

**Parameters**

`ip-address`—Specifies one of the IP addresses of the device.

**Command Mode**

Global Configuration mode

**User Guidelines**

To use this command, you must put the switch into routing mode using `set system`.

**Example**

The following example enters the IP interface configuration mode.

```plaintext
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)#
```

### 43 14  ip helper-address

Use the `ip helper-address` Global Configuration mode command to enable the forwarding of UDP Broadcast packets received on an interface to a specific (helper) address. Use the `no` form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

This command can only be used when the device is in Router mode.

**Syntax**

```plaintext
ip helper-address {ip-interface | all} address [udp-port-list]
no ip helper-address {ip-interface | all} address
```
Parameters

- **ip-interface**—Specifies the IP interface.
- **all**—Specifies all IP interfaces.
- **address**—Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- **udp-port-list**—Specifies the destination UDP port number to which to forward Broadcast packets. (Range: 1–65535). This can be a list of port numbers separated by spaces.

Default Configuration

Forwarding of UDP Broadcast packets received on an interface to a specific (helper) address is disabled.

If **udp-port-list** is not specified, packets for the default services are forwarded to the helper address.

Command Mode

Global Configuration mode

User Guidelines

To use this command, you must put the switch into routing mode using **set system**.

This command forwards specific UDP Broadcast packets from one interface to another, by specifying a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.
The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

**Example**

The following example enables the forwarding of UDP Broadcast packets received on all interfaces to the UDP ports of a destination IP address and UDP port 1 and 2.

```
switchxxxxxx(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

### 43 15  show ip helper-address

Use the `show ip helper-address` Privileged EXEC mode command to display the IP helper addresses configuration on the system.

This command can only be used when the device is in Router mode.

**Syntax**

```
show ip helper-address
```

**Parameters**

This command has no arguments or key words.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

To use this command, you must put the switch into routing mode using `set system`. 
Example

The following example displays the IP helper addresses configuration on the system.

```
switchxxxxxx# show ip helper-address
Interface       Helper Address     UDP Ports
----------------- --------------- --------------------------
192.168.1.1      172.16.8.8       37, 42, 49, 53, 137, 138
192.168.2.1      172.16.9.9       37, 49
```

43 16 show ip dhcp client interface

Use the `show ip dhcp client interface` command in User EXEC or Privileged EXEC mode to display DHCP client interface information.

Syntax

```
show ip dhcp client interface [interface-id]
```

Parameters

`interface-id`—Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

If no interfaces are specified, all interfaces on which DHCP client is enabled are displayed. If an interface is specified, only information about the specified interface is displayed.

Example

The following is sample output of the `show ip dhcp client interface` command:

```
show ip dhcp client interface
VLAN 100 is in client mode
    Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
```
Default Gateway: 170.10.100.1
DNS Servers: 115.1.1.1, 87.12.34.20
DNS Domain Search List: company.com
Host Name: switch_floor7
Configuration Server Addresses: 192.1.1.1 202.1.1.1
Configuration Path Name: qqq/config/aaa_config.dat
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
VLAN 1200 is in client mode
Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
Default Gateway: 180.10.100.1
DNS Servers: 115.1.1.1, 87.12.34.20
DNS Domain Search List: company.com
Host Name: switch_floor7
Configuration Server Addresses: configuration.company.com
Configuration Path Name: qqq/config/aaa_config.dat
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00

User Guidelines

If no interfaces are specified, all interfaces on which DHCP client is enabled are displayed. If an interface is specified, only information about the specified interface is displayed.

Example

The following is sample output of the `show ip dhcp client interface` command:

```
show ip dhcp client interface
VLAN 100 is in client mode
  Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
  Default Gateway: 170.10.100.1
  DNS Servers: 115.1.1.1, 87.12.34.20
  DNS Domain Search List: company.com
  Host Name: switch_floor7
  Configuration Server Addresses: 192.1.1.1 202.1.1.1
  Configuration Path Name: qqq/config/aaa_config.dat
```
POSIX Timezone string: EST5EDT4,M3.2.0/02:00, M11.1.0/02:00

VLAN 1200 is in client mode

Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192

Default Gateway: 180.10.100.1

DNS Servers: 115.1.1.1, 87.12.34.20

DNS Domain Search List: company.com

Host Name: switch_floor7

Configuration Server Addresses: configuration.company.com

Configuration Path Name: qqq/config/aaa_config.dat

POSIX Timezone string: EST5EDT4, M3.2.0/02:00, M11.1.0/02:00
IPv6 Router Commands

44.1 clear ipv6 neighbors

Use the clear ipv6 neighbors command in Privileged EXEC mode to delete all entries in the IPv6 neighbor discovery cache, except static entries.

Syntax

```
clear ipv6 neighbors
```

Parameters

N/A

Command Mode

Privileged EXEC

User Guidelines

Example

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
clear ipv6 neighbors
```

44.2 ipv6 address

Use the ipv6 address command in Interface Configuration mode to configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.

Use the no form of this command to remove the address from the interface.

Syntax

```
ipv6 address ipv6-address/prefix-length
no ipv6 address [ipv6-address/prefix-length]
```
Parameters

- **ipv6-address**—Specifies the IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- **prefix-length**—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). A slash mark must precede the decimal value.

**Default Configuration**

No IP address is defined for the interface.

**Command Mode**

Interface Configuration

**User Guidelines**

The `ipv6 address` command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the `no IPv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

**Example**

The following example defines the IPv6 global address 2001:DB8:2222:7272::72 on vlan 100:

```
interface vlan 100
  ipv6 address 2001:DB8:2222:7272::72/64

exit
```

### 44.3 ipv6 address autoconfig

Use the `ipv6 address autoconfig` command in Interface Configuration mode to enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.
Use the no form of this command to remove the address from the interface.

**Syntax**

ipv6 address autoconfig

no ipv6 address autoconfig

**Parameters**

N/A.

**Default Configuration**

Stateless Auto configuration is disabled.

**Command Mode**

Interface Configuration mode.

**User Guidelines**

This command enables IPv6 on an interface (if it was disabled) and causes the switch to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the eui-64 based addresses to the interface.

Stateless auto configuration is applied only when IPv6 Forwarding is disabled.

When IPv6 forwarding is changed from disabled to enabled, and stateless auto configuration is enabled the switch stops stateless auto configuration and removes all stateless auto configured ipv6 addresses from all interfaces.

When IPv6 forwarding is changed from enabled to disabled and stateless auto configuration is enabled the switch resumes stateless auto configuration.

Using the **no ipv6 address autoconfig** command to disable stateless auto configuration and to remove all stateless auto configured IPv6 addresses from an interface.

**Example**

The following example assigns the IPv6 address automatically:

```plaintext
interface vlan 100
  ipv6 address autoconfig
exit
```
44.4 **ipv6 address link-local**

Use the `ipv6 address link-local` command in Interface Configuration mode to configure an IPv6 link local address for an interface and enable IPv6 processing on the interface.

Use the `no` form of this command to remove the manually configured link local address from the interface.

**Syntax**

ipv6 address ipv6-prefix link-local

no ipv6 address [link-local]

**Parameters**

- **ipv6-address**—Specifies the IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

**Default Configuration**

The default Link-local address is defined.

**Command Mode**

Interface Configuration

**User Guidelines**

The switch automatically generates a link local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link local address to be used by an interface, use the `ipv6 address link-local` command.

The `ipv6 address link-local` command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the `no IPv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.
Example
The following example enables IPv6 processing on VLAN 1 and configures FE80::260:3EFF:FE11:6770 as the link local address for VLAN 1:

interface vlan 1
  ipv6 address FE80::260:3EFF:FE11:6770 link-local
exit

44.5 ipv6 default-gateway
Use the ipv6 default-gateway Global Configuration mode command to define an IPv6 default gateway.

Use the no form of this command to remove the default gateway.

Syntax
ipv6 default-gateway ipv6-address | interface-id
no ipv6 default-gateway ipv6-address | interface-id

Parameters
- ipv6-address—Specifies the IPv6 address of the next hop that can be used to reach a network.
- interface-id—Specifies the Interface Identifier of the outgoing interface that can be used to reach a network.

Default Configuration
No default gateway is defined.

Command Mode
Global Configuration mode

User Guidelines
The command is an alias of the ipv6 route command with the predefined (default) route:

ipv6 route ::/0 ipv6-address | interface-id
See the definition of the \texttt{ipv6 route} command for details.

**Example** The following example configures a default gateway:

```
console(config)# ipv6 default-gateway fe80::abcd%vlan1
```

### 44.6 ipv6 enable

Use the \texttt{ipv6 enable} command in Interface Configuration mode to enable IPv6 processing on an interface.

Use the \texttt{no} form of this command to disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

**Syntax**

```
ipv6 enable
no ipv6 enable
```

**Parameters**

N/A.

**Default Configuration**

IPv6 addressing is disabled.

**Command Mode**

Interface Configuration

**User Guidelines**

This command automatically configures an IPv6 link-local Unicast address on the interface while also enabling the interface for IPv6 processing. The \texttt{no ipv6 enable} command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

**Example**

The following example enables VLAN 1 for the IPv6 addressing mode.

```
interface vlan 1
  ipv6 enable
```
exit

44.7 ipv6 icmp error-interval

Use the `ipv6 icmp error-interval` command in Global Configuration mode to configure the interval and bucket size for IPv6 ICMP error messages.

Use the `no` form of this command to return the interval to its default setting.

Syntax

```
ipv6 icmp error-interval milliseconds [bucketsize]
```

```
no ipv6 icmp error-interval
```

Parameters

- `milliseconds`—Time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0 to 2147483647. A value of 0 disables ICMP rate limiting.
- `bucketsize`—Maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200.

Default Configuration

The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second.

Command Mode

Global Configuration mode

User Guidelines

Use this command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The `milliseconds` argument specifies the time interval between tokens arriving in the bucket. The optional `bucketsize` argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the `bucketsize` is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.
Average Packets Per Second = \( \frac{1000}{\text{milliseconds}} \times \text{bucketsize} \).

To disable ICMP rate limiting, set the \textit{milliseconds} argument to zero.

**Example**

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
ipv6 icmp error-interval 50 20
```

### 44.8 ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** command in Interface Configuration mode to configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the Unicast IPv6 addresses of the interface.

Use the **no** form of this command to return the number of messages to the default value.

**Syntax**

```
ipv6 nd dad attempts \textit{value}
```

```
no ipv6 nd dad attempts
```

**Parameters**

\textit{value}—The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

**Default Configuration**

1

**Command Mode**

Interface Configuration

**User Guidelines**

Duplicate address detection verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses
remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of Unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 4862, IPv6 Stateless Address Autoconfiguration) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface, while duplicate address detection is performed on a tentative Unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 4861, Neighbor Discovery for IPv6), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the `ipv6 nd ns-interval` command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the Unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

An interface returning to administratively up, restarts duplicate address detection for all of the Unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error SYSLOG message is issued.

If the duplicate address is a global address of the interface, the address is not used and an error SYSLOG message is issued.

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).
Example
The following example configures five consecutive neighbor solicitation messages to be sent on VLAN 1 while duplicate address detection is being performed on the tentative Unicast IPv6 address of the interface. The example also disables duplicate address detection processing on VLAN 2.

```plaintext
interface vlan 1
  ipv6 nd dad attempts 5
exit
interface vlan 2
  ipv6 nd dad attempts 0
exit
```

44.9 ipv6 neighbor
Use the `ipv6 neighbor` command in Global Configuration mode to configure a static entry in the IPv6 neighbor discovery cache.

Use the `no` form of this command to remove a static IPv6 entry from the IPv6 neighbor discovery cache.

Syntax
```plaintext
ipv6 neighbor ipv6-address interface-id mac-address
no ipv6 neighbor [[ipv6-address] interface-id]
```

Parameters
- `ipv6-address`—Specified IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- `interface-id`—Specified interface identifier.
- `mac-address`—Interface MAC address.

Default Configuration
Static entries are not configured in the IPv6 neighbor discovery cache.
Command Mode

Global Configuration

User Guidelines

This command is similar to the `arp` (global) command.

Use the `ipv6 neighbor` command to add a static entry in the IPv6 neighbor discovery cache.

If the specified IPv6 address is a global IPv6 address it must belong to one of static on-link prefixes defined in the interface. When a static on-link prefix is deleted all static entries in the IPv6 neighbor discovery cache corresponding the prefix is deleted to.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache, learned through the IPv6 neighbor discovery process, the entry is automatically converted to a static entry.

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Use the `no ipv6 neighbor ipv6-address interface-id` command to remove the one given static entry on the given interface. The command does not remove the entry from the cache, if it is a dynamic entry, learned from the IPv6 neighbor discovery process.

Use the `no ipv6 neighbor interface-id` command to delete the all static entries on the given interface.

Use the `no ipv6 neighbor` command to remove the all static entries on all interfaces.

Use the `show ipv6 neighbors` command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- NCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.

Note. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries.
Examples

Example 1—The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8:45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
ipv6 neighbor 2001:0DB8::45A vlan1 0002.7D1A.9472
```

Example 2—The following example deletes the static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8:45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
no ipv6 neighbor 2001:0DB8::45A vlan1
```

Example 3 —The following example deletes all static entries in the IPv6 neighbor discovery cache on VLAN 1:

```
no ipv6 neighbor vlan1
```

Example 4—The following example deletes all static entries in the IPv6 neighbor discovery cache on all interfaces:

```
no ipv6 neighbor
```

44.10 ipv6 unreachable

Use the `ipv6 unreachable` command in Interface Configuration mode to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.

Use the `no` form of this command to prevent the generation of unreachable messages.

Syntax

```
ipv6 unreachable
```

```
no ipv6 unreachable
```
Parameters
N/A.

Default Configuration
The sending of ICMP IPv6 unreachable messages is enabled.

Command Mode
Interface Configuration.

User Guidelines
If the switch receives a Unicast packet destined for itself that uses a protocol it
does not recognize, it sends an ICMPv6 unreachable message to the source.

If the switch receives a datagram that it cannot deliver to its ultimate destination
because it knows of no route to the destination address, it replies to the originator
of that datagram with an ICMP host unreachable message.

Example
The following example disables the generation of ICMPv6 unreachable messages,
as appropriate, on an interface:

```plaintext
interface vlan 100
  no ipv6 unreachables
exit
```

44.11 show ipv6 interface
Use the show ipv6 interface command in User EXEC or Privileged EXEC mode to
display the usability status of interfaces configured for IPv6.

Syntax

```
show ipv6 interface [brief] | [[interface-id] [prefix]]
```

Parameters

- **brief**—Displays a brief summary of IPv6 status and configuration for each
  interface where IPv6 is defined.
- **interface-id**—Interface identifier about which to display information.
- prefix—Prefix generated from a local IPv6 prefix pool.

Default Configuration

Option brief - all IPv6 interfaces are displayed.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use this command to validate the IPv6 status of an interface and its configured addresses. This command also displays the parameters that IPv6 uses for operation on this interface and any configured features.

If the interface's hardware is usable, the interface is marked up.

If you specify an optional interface identifier, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

Examples

Example 1—The show ipv6 interface command displays information about the specified interface:

```
show ipv6 interface vlan 1

VLAN 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
Global unicast address(es):
  Ipv6 Global Address Type
  2000:0DB8::2/64 (ANY) Manual
  2000:0DB8::2/64 Manual
  2000:1DB8::2011/64 Manual
Joined group address(es):
  FF02::1
  FF02::2
```
FF02::1:FF11:6770

MTU is 1500 bytes

ICMP error messages limited interval is 100ms; Bucket size is 10 tokens

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

Stateless autoconfiguration is enabled.

MLD Version is 2

Field Descriptions:

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked Enabled. If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked Stalled. If IPv6 is not enabled, the interface is marked Disabled.
- **link-local address**—Displays the link-local address assigned to the interface.
- **Global unicast address(es):**—Displays the global Unicast addresses assigned to the interface. The type is **manual** or **autoconfig**.
- **Joined group address(es):**—Indicates the Multicast groups to which this interface belongs.
- **Maximum transmission unit of the interface.**
- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled).
- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
Example 2—The show ipv6 interface command displays information about the specified manual IPv6 tunnel:

```
show ipv6 interface tunnel 2
Tunnel 2 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
Global unicast address(es):
  Ipv6 Global Address                         Type
  2000:0DB8::2/64   (ANY)                     Manual
  2000:0DB8::2/64                     Manual
  2000:1DB8::2011/64                  Manual
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF11:6770
MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
MLD Version is 2
Tunnel mode is manual
Tunnel Local IPv4 address : 10.10.10.1(auto)
Tunnel Remote Ipv4 address : 10.1.1.1
```

**Field Descriptions:**

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the
interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”

- **link-local address**—Displays the link-local address assigned to the interface.

- **Global Unicast address(es):**—Displays the global Unicast addresses assigned to the interface. The type is **manual** or **autoconfig**.

- **Joined group address(es):**—Indicates the Multicast groups to which this interface belongs.

- **—Maximum transmission unit of the interface.**

- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.

- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled).

- **number of DAD attempts**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

- **MLD Version**—The version of MLD

- **Tunnel mode**—Specifies the tunnel mode: **manual**, **6to4**, **auto-tunnel** or **isatap**

- **Tunnel Local IPv4 address**—Specifies the tunnel local IPv4 address and have one of the following formats:
  - `ipv4-address`
  - `ipv4-address (auto)`
  - `ipv4-address (interface-id)`

- **Tunnel Remote IPv4 address**—Specifies the tunnel remote IPv4 address

---

**Example 3.** The **show ipv6 interface** command displays information about the specified ISATAP tunnel:
**show ipv6 interface tunnel 1**

Tunnel 1 is up/up

IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01

Global unicast address(es):

<table>
<thead>
<tr>
<th>IPv6 Global Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:0DB8::2/64 (ANY)</td>
<td>Manual</td>
</tr>
<tr>
<td>2000:0DB8::2/64</td>
<td>Manual</td>
</tr>
<tr>
<td>2000:1DB8::2011/64</td>
<td>Manual</td>
</tr>
</tbody>
</table>

Joined group address(es):

| FF02::1                           |
| FF02::2                           |
| FF02::1:FF11:6770                 |

is 1500 bytes

ICMP error messages limited interval is 100ms; Bucket size is 10 tokens

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

MLD Version is 2

Tunnel mode is ISATAP

Tunnel Local IPv4 address : 10.10.10.1(VLAN 1)

ISATAP Router DNS name is isatap

**Field Descriptions:**

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.

- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”

- **link-local address**—Displays the link-local address assigned to the interface.
Global Unicast address(es):—Displays the global Unicast addresses assigned to the interface. The type is manual or autoconfig.

Joined group address(es):—Indicates the Multicast groups to which this interface belongs.

—Maximum transmission unit of the interface.

ICMP error messages—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.

ND DAD—The state of duplicate address detection on the interface (enabled or disabled).

number of DAD attempts:—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

ND reachable time—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

MLD Version—The version of MLD

Tunnel mode—Specifies the tunnel mode: manual, 6to4, auto-tunnel or isatap

Tunnel Local IPv4 address—Specifies the tunnel local IPv4 address and have one of the following formats:
- ipv4-address
- ipv4-address (auto)
- ipv4-address (interface-id)

Tunnel Remote IPv4 address—Specifies the tunnel remote IPv4 address

ISATAP Router DNS name is—The DNS name of the ISATAP Router

Example 4. The following command with the brief keyword displays information about all interfaces that IPv6 is defined on:

```
Router# show ipv6 interface brief
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface IPv6 State</th>
<th>Link Local IPv6 Address</th>
<th>MLD Version</th>
<th>Number of Global Addresses</th>
</tr>
</thead>
</table>

78-21075-01 Command Line Interface Reference Guide
Example 5. This sample output shows the characteristics of VLAN 1 that has generated a prefix from a local IPv6 prefix pool:

interface vlan 1
  ipv6 address 2001:0DB8:1::1/64
  ipv6 address 2001:0DB8:2::1/64
  ipv6 address 2001:0DB8:3::1/64
  ipv6 nd prefix 2001:0DB8:1::/64 no-advertise
  ipv6 nd prefix 2001:0DB8:3::/64 2912000 564900 off-link
  ipv6 nd prefix 2001:0DB8:4::/64
  ipv6 nd prefix 2001:0DB8:5::/64 2912000 564900 off-link
exit
.
.
.show ipv6 interface vlan 1 prefix
IPv6 Prefix Advertisements VLAN 1
Codes: A - Address, P - Prefix is advertised, R is in Routing Table

<table>
<thead>
<tr>
<th>Code</th>
<th>Prefix</th>
<th>Flags</th>
<th>Valid Lifetime</th>
<th>Preferred Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>default</td>
<td>LA</td>
<td>2592000</td>
<td>604800</td>
</tr>
<tr>
<td>AR</td>
<td>2001:0DB8:1::/64</td>
<td>LA</td>
<td>infinite</td>
<td>infinite</td>
</tr>
</tbody>
</table>
### show ipv6 neighbors

Use the `show ipv6 neighbors` command in User EXEC or Privileged EXEC mode to display IPv6 neighbor discovery (ND) cache information.

**Syntax**

```
show ipv6 neighbors [interface-id | ipv6-address | ipv6-hostname]
```

**Parameters**

- **interface-id**—Specifies the identifier of the interface from which IPv6 neighbor information is to be displayed.

- **ipv6-address**—Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- **ipv6-hostname**—Specifies the IPv6 host name of the remote networking device.

**Default Configuration**

All IPv6 ND cache entries are listed.

**Command Mode**

User EXEC

Privileged EXEC

**User Guidelines**

When the `interface-id` argument is not specified, cache information for all IPv6 neighbors is displayed. Specifying the `interface-id` argument displays only cache information about the specified interface.
Examples

**Example 1**—The following is sample output from the `show ipv6 neighbors` command when entered with an interface-id:

```
show ipv6 neighbors vlan 1
```

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Age</th>
<th>Link-layer Addr</th>
<th>State</th>
<th>Interface</th>
<th>Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:0:4::2</td>
<td>0</td>
<td>0003.a0d6.141e</td>
<td>REACH</td>
<td>VLAN1</td>
<td>Yes</td>
</tr>
<tr>
<td>3001:1::45a</td>
<td>-</td>
<td>0002.7d1a.9472</td>
<td>REACH</td>
<td>VLAN1</td>
<td>-</td>
</tr>
<tr>
<td>FE80::203:A0FF:FED6:141E</td>
<td>0</td>
<td>0003.a0d6.141e</td>
<td>REACH</td>
<td>VLAN1</td>
<td>No</td>
</tr>
</tbody>
</table>

**Example 2**—The following is sample output from the `show ipv6 neighbors` command when entered with an IPv6 address:

```
show ipv6 neighbors 2000:0:4::2
```

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Age</th>
<th>Link-layer Addr</th>
<th>State</th>
<th>Interface</th>
<th>Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:0:4::2</td>
<td>0</td>
<td>0003.a0d6.141e</td>
<td>REACH</td>
<td>VLAN1</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Field Descriptions:**

- **Total number of entries**—Number of entries (peers) in the cache.
- **IPv6 Address**—IPv6 address of neighbor or interface.
- **Age**—Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- **Link-layer Addr**—MAC address. If the address is unknown, a hyphen (-) is displayed.
- **Interface**—Interface which the neighbor is connected to.
- **Router**—Specifies if the neighbor is a Router. A hyphen (-) is displayed for static entries.

### 44.13 show ipv6 route

Use the `show ipv6 route` command in user EXEC or privileged EXEC mode to display the current contents of the IPv6 routing table.
Syntax

show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol | interface interface-id]

Parameters

- **ipv6-address**—Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- **ipv6-prefix**—Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- **/prefix-length**—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). A slash mark must precede the decimal value.

- **protocol**—Displays routes for the specified routing protocol using the keyword: rip or one of the following.
  - **local**—Displays local routes.
  - **connected**—Displays connected routes.
  - **static**—Displays static routes.
  - **icmp**—Displays ICMP routes.
  - **nd**—Displays router advertisements.

- **interface interface-id**—Identifier of an interface whose routes are displayed.

Default Configuration

All IPv6 routing information for all active routing tables is displayed.

Command Mode

User EXEC
Privileged EXEC
User Guidelines

This command provides output similar to the `show ip route` command, except that the information is IPv6-specific.

When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed.

When the `icmp, nd, connected, local, or static` keywords are specified, only that type of route is displayed. When the `interface-id` argument are specified, only the specified interface-specific routes are displayed.

Examples

Example 1—The following is sample output from the `show ipv6 route` command when IPv6 Routing is not enabled and the command is entered without an IPv6 address or prefix specified:

```
show ipv6 route
Codes: > - Best
        S - Static, I - ICMP Redirect, ND - Router Advertisement
[d/m]: d - route’s distance, m - route’s metric
IPv6 Routing Table - 6 entries
S> ::/0 [1/1]
   via fe80::77  VLAN 1
ND> ::/0  [11/0]
     via fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
ND> 2001::/64  [0/0]
     via ::  VLAN 100
ND> 2002:1:1:1::/64  [0/0]
     via ::  VLAN 100
ND> 3001::/64  [0/0]
     via ::  VLAN 101
ND> 4004::/64  [0/0]
     via ::  VLAN 110
```
Example 2—The following is sample output from the `show ipv6 route` command when IPv6 Routing is supported and the command is entered without an IPv6 address or prefix specified and IPv6 Routing is enabled:

```
show ipv6 route
Codes: > - Best
       I - ICMP Redirect, S - Static, C - Connected,
       L - Local(on-link prefixes defined by the `ipv6 nd prefix` command with `on-link` keyword,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
[d/m]: d - route’s distance, m - route’s metric
IPv6 Routing Table - 5 entries
B>   3000::/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00   VLAN 100
OE1> 4000::2/128 [0/0]
     via FE80::A8BB:CCFF:FE02:8B01   VLAN 101
O>   4000::/64 [0/0]
     via FE80::A8BB:CCFF:FE02:8B02   VLAN 101
C>   4001::/64 [0/0]
     via ::   VLAN 100
L>   4002::/64 [0/0]
     via ::   VLAN 100 Lifetime 9000 sec
```

Example 3—The following is sample output from the `show ipv6 route` command when entered with the IPv6 prefix 2001:200::/35 and IPv6 Routing is supported:

```
show ipv6 route 2001:200::/35
Codes: > - Best
       I - ICMP Redirect, S - Static, C - Connected,
       L - Local(on-link prefixes defined by the `ipv6 nd prefix` command with `on-link` keyword,
```
O - OSPF intra-area, OIA - OSPF inter-area,
OE1 - OSPF external 1, OE2 - OSPF external 2,
[d/m]: d - route’s distance, m - route’s metric
IPv6 Routing Table - 261 entries
OE1> 2001:200::/35 [20/3]
       via FE80::60:5C59:9E00:16 Tunnel1
Tunnel Commands

45.1 interface tunnel

Use the interface tunnel Global Configuration mode command to enter the Interface Configuration (Tunnel) mode.

Syntax

interface tunnel number

Parameters

number— Specifies the tunnel number.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

The following example enters the Interface Configuration (Tunnel) mode.

```
interface tunnel 1
  tunnel source auto
exit
```

45.2 tunnel isatap solicitation-interval

Use the tunnel isatap solicitation-interval Global Configuration mode command to set the time interval between unsolicited router solicitation messages. Use the no form of this command to restore the default configuration.

Syntax

tunnel isatap solicitation-interval seconds

no tunnel isatap solicitation-interval
Parameters

seconds— Specifies the time interval in seconds between ISATAP router solicitation messages. (Range: 10–3600)

Default Configuration

The default time interval between ISATAP router solicitation messages is 10 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command determines the interval between unsolicited router solicitation messages sent to discovery an ISATAP router.

Example

The following example sets the time interval between ISATAP router solicitation messages to 30 seconds.

```
tunnel isatap solicitation-interval 30
```

45.3 tunnel isatap robustness

Use the tunnel isatap robustness Global Configuration mode command to configure the number of router solicitation refresh messages that the device sends. Use the no form of this command to restore the default configuration.

Syntax

```
tunnel isatap robustness number
no tunnel isatap robustness
```

Parameters

number— Specifies the number router solicitation refresh messages that the device sends. (Range: 1–20)
Default Configuration
The default number of router solicitation refresh messages that the device sends is 3.

Command Mode
Global Configuration mode

User Guidelines
The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router, divided by (Robustness + 1).

Example
The following example sets the number of router solicitation refresh messages that the device sends to 5.

```
tunnel isatap robustness 5
```

45.4 tunnel isatap router
Use the tunnel isatap router Interface Configuration (Tunnel) mode command to configure a global string that represents a specific automatic tunnel router domain name. Use the no form of this command to remove this router name and restore the default configuration.

Syntax
```
tunnel isatap router router-name
```

no tunnel isatap router

Parameters
`router-name`— Specifies the router’s domain name.

Default Configuration
The automatic tunnel router's default domain name is ISATAP.

Command Mode
Interface Configuration (Tunnel) mode
User Guidelines

This command determines the string that the host uses for automatic tunnel router lookup in the IPv4 DNS procedure. By default, the string ISATAP is used for the corresponding automatic tunnel types.

Only one string can represent the automatic tunnel router name per tunnel. Using this command, therefore, overwrites the existing entry.

The empty string means that automatic lookup is not applied.

Example

The following example configures the global string ISATAP2 as the automatic tunnel router domain name.

```
interface tunnel 1
  tunnel isatap router ISATAP2
exit
```

45.5 tunnel mode ipv6ip

Use the `tunnel mode ipv6ip` command in Interface Configuration mode to configure a static IPv6 tunnel interface. To remove an IPv6 tunnel interface, use the `no` form of this command.

Syntax

```
tunnel mode ipv6ip {isatap}
no tunnel mode ipv6ip
```

Parameters

- `isatap`—Specifies IPv6 automatic tunneling mode as ISATAP to connect IPv6 nodes (hosts and routers) within IPv4 networks.

Default Configuration

IPv6 tunnel interfaces are not configured.

Command Mode

Tunnel Interface Configuration
**User Guidelines**

IPv6 tunneling consists of encapsulating IPv6 packets within IPv4 packets for transmission across an IPv4 routing infrastructure.

**ISATAP Tunnels**

Using this command with the `isatap` keyword specifies automatic ISATAP tunnel. ISATAP tunnels enable transport of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

Unlike IPv4-compatible addresses, ISATAP IPv6 addresses can use any initial Unicast /64 prefix. The final 64 bits are an interface identifier. Of these, the leading 32 bits are the fixed pattern 0000:5EFE; the last 32 bits carry the tunnel endpoint IPv4 address.

**Example**

**Example 1** - The following example configures a ISATAP tunnel:

```plaintext
interface tunnel 1
  tunnel mode ipv6ip isatap
exit
```

**45.6 tunnel source**

Use the `tunnel source` Interface Configuration (Tunnel) mode command to set the local (source) IPv4 address of a tunnel interface. The `no` form deletes the tunnel local address.

**Syntax**

```
tunnel source {auto | ipv4-address | interface-id}
no tunnel source
```

**Parameters**

- **auto**—The system minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the IPv4 address is changed, then the local address of the tunnel interface is changed too.

- **ipv4-address**—Specifies the IPv4 address to use as the source address for packets sent on the tunnel interface. The local address of the tunnel
interface is not changed when the IPv4 address is moved to another interface

- **interface-id**—Interface which the minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the minimum IPv4 address is removed from the interface (removed at all, moved to another interface) then the next minimum IPv4 address is chosen as the local IPv4 address.

**Default**

No source address is defined.

**Command Mode**

Interface Configuration (Tunnel) mode

**User Guidelines**

The configured source IPv4 address is used for forming the tunnel interface identifier. The interface identifier is set to the 8 least significant bytes of the SIP field of the encapsulated IPv6 tunneled packets.

**Example**

```
interface tunnel 1
  tunnel source auto
exit
```

### 45.7 show ipv6 tunnel

Use the `show ipv6 tunnel` EXEC mode command to display information on the ISATAP tunnel.

**Syntax**

```
show ipv6 tunnel [all]
```

**Parameters**

- **all**— The switch displays all parameters of the tunnel. If the keyword is not configured only the tunnel parameters corresponding to its type are displayed.
Command Mode

EXEC mode

Example

Example 1. The following example displays information on the ISATAP tunnel, when the all keyword is not configured:

```
switchxxxxxx# show ipv6 tunnel
Tunnel 1
  Tunnel type          : ISATAP
  Tunnel status        : UP
  Tunnel Local address type : VLAN 100
  Tunnel Local Ipv4 address : 192.1.3.4
  Tunnel Remote Ipv4 address : 192.3.4.5
Tunnel 2
  Tunnel type          : ISATAP
  Tunnel status        : UP
  Tunnel Local address type : auto
  Tunnel Local Ipv4 address : 192.1.3.4
  Router DNS name               : ISATAP
  Router IPv4 addresses
    1.1.1.1          Detected
    100.1.1.1        Detected
    14.1.100.1       Not Detected
  Router Solicitation interval : 10 seconds
  Robustness               : 2
```

Example 2. The following example displays information when the all keyword is configured:

```
switchxxxxxx# show ipv6 tunnel all
Tunnel 1
```
Tunnel type                      : ISATAP  
Tunnel status                    : UP  
Tunnel Local address type        : VLAN 100  
Tunnel Local Ipv4 address        : 192.1.3.4  
ISATAP Parameters  
  Router DNS name                : ISATAP  
  Router Solicitation interval   : 10 seconds  
  Robustness                     : 2  

Tunnel 2  
Tunnel type                      : ISATAP  
Tunnel status                    : UP  
Tunnel Local address type        : auto  
ISATAP Parameters  
  Tunnel Local Ipv4 address      : 192.1.3.4  
  Router DNS name                : ISATAP  
  Router IPv4 addresses  
    1.1.1.1          Detected  
    100.1.1.1        Detected  
    14.1.100.1       Not Detected  
  Router Solicitation interval   : 10 seconds  
  Robustness                     : 2
DHCP Relay Commands

46.1  ip dhcp relay enable (Global)

Use the `ip dhcp relay enable` Global Configuration mode command to enable the DHCP relay feature on the device. Use the `no` form of this command to disable the DHCP relay feature.

**Syntax**

```
ip dhcp relay enable
no ip dhcp relay enable
```

**Parameters**

N/A

**Default Configuration**

DHCP relay feature is disabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables the DHCP relay feature on the device.

```
switchxxxxxx(config)# ip dhcp relay enable
```

46.2  ip dhcp relay enable (Interface)

Use the `ip dhcp relay enable` Interface Configuration (VLAN, Ethernet, Port-channel) mode command to enable the DHCP relay feature on an interface. Use the `no` form of this command to disable the DHCP relay agent feature on an interface.
DHCP Relay Commands

### Syntax

```
ip dhcp relay enable
no ip dhcp relay enable
```

### Parameters

N/A

### Default Configuration

Disabled

### Command Mode

Interface Configuration (VLAN, Ethernet, Port-channel) mode

### User Guidelines

The operational status of DHCP Relay on an interface is active if one of the following conditions exist:

- DHCP Relay is globally enabled, and there is an IP address defined on the interface.
- Or
  - DHCP Relay is globally enabled, there is no IP address defined on the interface, the interface is a VLAN, and option 82 is enabled.

### Example

The following example enables DHCP Relay on VLAN 21.

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay enable
```

### 46.3 ip dhcp relay address (Global)

Use the `ip dhcp relay address` Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the `no` form of this command to remove the server from the list.
DHCP Relay Commands

Syntax

ip dhcp relay address ip-address
no ip dhcp relay address [ip-address]

Parameters

ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the ip dhcp relay address command to define a global DHCP Server IP address. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all global defined DHCP servers.

Example

The following example defines the DHCP server on the device.

switchxxxxxx(config)# ip dhcp relay address 176.16.1.1

46.4  ip dhcp relay address (Interface)

Use the ip dhcp relay address Interface Configuration (VLAN, Ethernet, Port-channel) command to define the DHCP servers available by the DHCP relay for DHCP clients connected to the interface. Use the no form of this command to remove the server from the list.

Syntax

ip dhcp relay address ip-address
no ip dhcp relay address [ip-address]

Parameters

ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Interface Configuration (VLAN, Ethernet, Port-channel) mode

User Guidelines

Use the ip dhcp relay address command to define a DHCP Server IP address per the interface. To define multiple DHCP Servers, use the command multiple times.

Before using this command, set the device in router mode with the command set system mode.

To remove a DHCP Server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all DHCP servers defined per the interface.

You can use the command regardless if DHCP Relay is enabled on the interface.

Example

The following example defines the DHCP server on the device.

switchxxxxxx(config)# ip dhcp relay address 176.16.1.1

46.5 show ip dhcp relay

Use the show ip dhcp relay EXEC mode command to display the DHCP relay information.

Syntax

show ip dhcp relay
**Command Mode**

**EXEC mode**

**Examples**

**Example 1 - Option 82 is not supported:**

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

**Example 2 - Option 82 is supported (disabled):**

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: gi5,po3-4
  Active:
  Inactive: gi5, po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active:
  Inactive: 1, 2, 4, 5
Global Servers: 1.1.1.1 , 2.2.2.2
```
Example 3. Option 82 is supported (enabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi5,po3-4
  Active: gi5
  Inactive: po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active: 1, 2, 4, 5
  Inactive:
Global Servers: 1.1.1.1, 2.2.2.2
```

Example 3. Option 82 is supported (enabled) and there DHCP Servers defined per interface:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi5,po3-4
  Active: gi5
  Inactive: po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active: 1, 2, 4, 5
  Inactive:
Global Servers: 1.1.1.1, 2.2.2.2
VLAN 1: 1.1.1.1, 100.10.1.1
```
46.6  ip dhcp information option

Use the ip dhcp information option Global Configuration command to enable DHCP option-82 data insertion. Use the no form of this command to disable DHCP option-82 data insertion.

Syntax

ip dhcp information option

no ip dhcp information option

Parameters

N/A

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

switchxxxxxx(config)\# ip dhcp information option

46.7  show ip dhcp information option

The show ip dhcp information option EXEC mode command displays the DHCP Option 82 configuration.

Syntax

show ip dhcp information option
**Parameters**

N/A

**Default Configuration**

N/A

**Command Mode**

EXEC mode

**Example**

The following example displays the DHCP Option 82 configuration.

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
```
### 47.1 ip route

Use the `ip route` command in Global Configuration mode to establish static routes.

Use the `no` form of this command to remove static routes.

**Syntax**

```
ip route prefix {mask | /prefix-length} {{ip-address [metric cost]} | reject-route}
no ip route prefix {mask | prefix-length} [ip-address]
```

**Parameters**

- `prefix`—IP route prefix for the destination.
- `mask`—Prefix mask for the destination.
- `/prefix-length`—Prefix mask for the destination. Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- `ip-address`—IP address of the next hop that can be used to reach that network.
- `reject-route`—Stops routing to the destination network via all gateways.
- `metric cost`—Cost (metric) of the route. The default cost is 1. Range: 1–255.

**Default Configuration**

No static routes are established. The default metric cost is 1.

**Command Mode**

Global configuration (config)

**User Guidelines**

Use the `no ip route` command without the `ip-address` parameter to remove all static routes to the given subnet.

Use the `no ip route` command with the `ip-address` parameter to remove only one static route to the given subnet via the given next hop.
Example

**Example 1** - The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

**Example 2** - The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length:

```
ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

**Example 3** - The following example shows how to reject packets for network 194.1.1.0:

```
ip route 194.1.1.0 255.255.255.0 reject-route
```

**Example 4** - The following example shows how to remove all static routes to network 194.1.1.0/24:

```
no ip route 194.1.1.0 /24
```

**Example 5** - The following example shows how to remove one static route to network 194.1.1.0/24 via 1.1.1.1:

```
no ip route 194.1.1.0 /24 1.1.1.1
```

### 47.2 show ip route

Use the `show ip route` command in user EXEC or privileged EXEC mode to display the current state of the routing table.

**Syntax**

```
show ip route [address IP_address{mask [longer-prefixes]] | [static | rejected | connected | summary]
```
Parameters

- **address IP_address**—IP address about which routing information should be displayed.
- **mask**—The subnet mask.
- **longer-prefixes**—Specifies that only routes matching the IP address and mask pair should be displayed.
- **static**—Displays static routes only.
- **connected**—Displays connected routes only.
- **rejected**—Displays rejected routes only.
- **summary**—Displays current contents of the IP routing table in summary format.

Example

**Example 1** - The following is sample output from this command when IP Routing is not enabled:

```
Router# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: disabled
```

**Example 2** - The following is sample output from this command when IP Routing is enabled:

```
SG300-10SFP-L3#show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled
Codes: > - best, C - connected, S - static
S  0.0.0.0/0 [1/1] via 10.5.234.254, 25:7:2, vlan 1
C  10.5.234.0/24 is directly connected, vlan 1
```
48.1  ip access-list (IP extended)

Use the **ip access-list extended** Global Configuration mode command to name an IPv4 access list (ACL) and to place the device in IPv4 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the `permit (IP)` and `deny (IP)` commands. The `service-acl input` command is used to attach this ACL to an interface.

Use the **no** form of this command to remove the access list.

**Syntax**

```
ip access-list extended acl-name
no ip access-list extended acl-name
```

**Parameters**

- **acl-name**—Name of the IPv4 access list. (Range 1-32 characters)

**Default Configuration**

No IPv4 access list is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

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

**Example**

```bash
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)#
```
48.2 permit (IP)

Use the permit IP Access-list Configuration mode command to set permit conditions for an IPv4 access list (ACL). Permit conditions are also known as access control entries (ACEs).

Syntax

```
permit protocol [any | source source-wildcard] [any | destination destination-wildcard] [dscp number | precedence number] [time-range time-range-name]
```

```
permit icmp [any | source source-wildcard] [any | destination destination-wildcard] [any | icmp-type] [any | icmp-code] [dscp number | precedence number] [time-range time-range-name]
```

```
permit igmp [any | source source-wildcard] [any | destination destination-wildcard] [igmp-type] [dscp number | precedence number] [time-range time-range-name]
```

```
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] [time-range time-range-name]
```

```
permit udp [any | source source-wildcard] [any | source-port/port-range] [any | destination destination-wildcard] [any | destination-port/port-range] [dscp number | precedence number] [time-range time-range-name]
```

Parameters

- **permit protocol**—The name or the number of an IP protocol. Available protocol names are: icmp, igmp, ip, tcp, egp, igrp, udp, hmp, rdp, idpr, ipv6, ipv6:icm, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the ip keyword (Range: 0–255)
- **source**—Source IP address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.
- **destination**—Destination IP address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.
- **dscp number**—Specifies the DSCP value.
- **precedence number**—Specifies the IP precedence value.
### ACL Commands

- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following 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, photuris. (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)

- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)

- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 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), klogin (543), kshell (544), ldp (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), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177),(Range: 0–65535).

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—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 a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

### Default Configuration

No IPv4 access list is defined.
Command Mode
IP Access-list Configuration mode

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

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

Example

```
switchxxxxxxx(config)# ip access-list extended server
switchxxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255
```

48.3 deny (IP)
Use the `deny` IP Access-list Configuration mode command to set deny conditions for IPv4 access list. Deny conditions are also known as access control entries (ACEs).

Syntax

```
deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name]
deny icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code] [dscp number | precedence number] <all but Cisco> [time-range time-range-name]
deny igmp {any | source source-wildcard} {any | destination destination-wildcard} [igmp-type] [dscp number | precedence number] <all but Cisco> [time-range time-range-name]
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] <all but Cisco> [time-range time-range-name]
```
deny udp {any | source source-wildcard} {any | source-port/port-range} {any | destination destination-wildcard} {any | destination-port/port-range} [dscp number | precedence number] [time-range time-range-name]

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igrp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, I2tp, isis. To match any protocol, use the lp keyword. (Range: 0–255)

- **source**—Source IP address of the packet.

- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.

- **destination**—Destination IP address of the packet.

- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.

- **dscp number**—Specifies the DSCP value.

- **precedence number**—Specifies the IP precedence value.

- **icmptype**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following 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, photuris. (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)

- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)

- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 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), ldap (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-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—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 a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

- **disable-port**—The Ethernet interface is disabled if the condition is matched.

- **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

**Default Configuration**

No IPv4 access list is defined.

**Command Mode**

IP Access-list Configuration mode

**User Guidelines**

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

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

**Example**
switchxxxxx(config)# ip access-list extended server
switchxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255

48.4  ipv6 access-list (IPv6 extended)

Use the ipv6 access-list Global Configuration mode command to define an IPv6 access list (ACL) and to place the device in IPv6 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the permit (IPv6) and deny (IPv6) commands. The service-acl input command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax

ipv6 access-list [acl-name]

no ipv6 access-list [acl-name]

Parameters

acl-name—Name of the IPv6 access list. Range 1-32 characters.

Default Configuration

No IPv6 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Every IPv6 ACL has an 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 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 ACLs implicitly allow ARP packets to be sent and received on an interface.
Example

Switch (config)# ipv6 access-list acl1
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any any 80

48.5 permit (IPv6)

Use the `permit` command in IPv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs.

Syntax

```
permit protocol {any | {source-prefix/length}{any | destination-prefix/length}} [dscp number | precedence number] [time-range time-range-name]
permit icmp {any | {source-prefix/length}{any | destination-prefix/length}} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [all but Cisco> [time-range time-range-name]
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] [all but Cisco> [time-range time-range-name]
permit udp {any | {source-prefix/length}} {any | source-port/port-range} {any | destination-prefix/length} {any | destination-port/port-range} [dscp number | precedence number] [all but Cisco> [time-range time-range-name]
```

Parameters

- **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: 0–255)
- **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.
- **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.
- **dscp number**—Specifies the DSCP value. (Range: 0–63)
- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following 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), nd-na (136). (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 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+ (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), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flag**—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 a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

**Default Configuration**

No IPv6 access list is defined.

**Command Mode**

IPv6 Access-list Configuration mode
User Guidelines

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

The number of TCP/UDP ranges that can be defined in ACLs is limited. 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 destination port in ACE it is not counted again if it is also used for destination port in another ACE.

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

Example

This example defines an ACL by the name of server and enters a rule (ACE) for tcp packets.

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

48.6 deny ( IPv6 )

Use the `deny` command in IPv6 Access List Configuration mode to set permit conditions (ACEs) for IPv6 ACLs.

Syntax

```
deny protocol {any | [source-prefix/length]}{any | destination-prefix/length} [dscp number | precedence number][time-range time-range-name] [disable-port / log-input]

deny icmp {any | [source-prefix/length]}{any | destination-prefix/length} [any | icmp-type] [any | icmp-code] [dscp number | precedence number][time-range time-range-name] [disable-port / log-input]

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][time-range time-range-name] [disable-port / log-input]

deny udp {any | [source-prefix/length]}{any | source-port/port-range}{any | destination-prefix/length} [any | destination-port/port-range] [dscp number | precedence number][time-range time-range-name] [disable-port / log-input]
```
**Parameters**

- **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: 0–255)

- **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.

- **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.

- **dscp number**—Specifies the DSCP value. (Range: 0–63)

- **precedence number**—Specifies the IP precedence value.

- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following 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), nd-na (136). (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)

- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 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 (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), xdmcp (177). (Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flags**—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 a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

- **disable-port**—The Ethernet interface is disabled if the condition is matched.

- **log-input**—Specifies to send an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

**Default Configuration**

No IPv6 access list 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. If a range of ports is used for source port in ACE it is not counted again if it is also used for 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 source port it is counted again if it is also used for destination port.

**Example**

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

### 48.7 **mac access-list**

Use the **mac access-list** Global Configuration mode command to define a Layer 2 access list (ACL) based on source MAC address filtering and to place the device in MAC Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the **permit (MAC)** and
deny (MAC) commands. The **service-acl input** command is used to attach this ACL to an interface.

Use the **no** form of this command to remove the access list.

**Syntax**

```plaintext
mac access-list extended acl-name
no mac access-list extended acl-name
```

**Parameters**

- **acl-name**—Specifies the name of the MAC ACL (Range: 1–32 characters).

**Default Configuration**

No MAC access list is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

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

**Example**

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

### 48.8 permit ( MAC )

Use the **permit** command in MAC Access List Configuration mode to set permit conditions (ACEs) for a MAC ACL.

**Syntax**

```plaintext
permit {any | source source-wildcard} {any | destination destination-wildcard} 
[eth-type 0 | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos-wildcard]
```
ACL Commands

/time-range time-range-name/

Parameters

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094)
- **cos**—The Class of Service of the packet. (Range: 0–7)
- **cos-wildcard**—Wildcard bits to be applied to the CoS.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

User Guidelines

After an access control entry (ACE) is added to an access control list, 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-al)# permit 00:00:00:00:01 00:00:00:ff any
```
48.9 deny (MAC)

Use the **deny** command in MAC Access List Configuration mode to set deny conditions (ACEs) for a MAC ACL.

**Syntax**

```
deny {any | source source-wildcard} {any | destination destination-wildcard} 
[eth-type 0] | aarp | amber | dec-spanning | deenet-iv | diagnostic | dsm | etype-6000 | vlan vlan-id | [cos cos-wildcard] [time-range time-range-name] 
[disable-port | log-input]
```

**Parameters**

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use ones in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094)
- **cos**—The Class of Service of the packet. (Range: 0–7)
- **cos-wildcard**—Wildcard bits to be applied to the CoS.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Sends an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

**Default Configuration**

No MAC access list is defined.
Command Mode
MAC Access-list Configuration mode

User Guidelines
After an access control entry (ACE) is added to an access control list, 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-al)# deny 00:00:00:00:00:01 00:00:00:00:ff any
```

48.10 service-acl input
Use the service-acl input command in interface Configuration mode to bind an access list(s) (ACL) to an interface.

Use the no form of this command to remove all ACLs from the interface.

Syntax
```
service-acl input acl-name1 [acl-name2] default-action {deny-any | permit-any}
no service-acl input
```

Parameters
- **acl-name**—Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).
- **permit-any**—If the packet does not match the ACL criteria, it is forwarded by default.
- **deny-any**—If the packet does not match the ACL criteria, it is dropped by default.

Default Configuration
No ACL is assigned.
Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.

User Guidelines

The following rules govern when ACLs can be bound or unbound from an interface:

- IPv4 ACLs and IPv6 ACLs can be bound together to an interface.
- A MAC ACL cannot be bound on an interface which already has an IPv4 ACL or IPv6 ACL bound to it.
- Two ACLs of the same type cannot be bound to a port.
- An ACL cannot be bound to a port that is already bound to an ACL, without first removing the current ACL. Both ACLs must be mentioned at the same time in this command.

Example

```
switchxxxxxx(config)# mac access-list extended server-acl
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

48.11 time-range

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

This command sets a time-range name. Use the absolute and periodic commands to actually configure the time-range.

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

Syntax

time-range time-range-name

no time-range time-range-name
Parameters

time-range-name—Specifies the name for the time range. (Range: 1–32 characters)

Default Configuration

No time range is defined

Command Mode

Global Configuration mode

User Guidelines

After adding the name of a time range with this command, use the **absolute** and **periodic** commands to actually configure the time-range. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range ACEs are not activated.

The user cannot delete a time-range that is bound to any features, such as ACLs.

When a time range is defined, it can be used in the following commands:

- `dot1x port-control`
- `power inline`
- `permit (IP)`
- `deny (IP)`
- `permit (IPv6)`
- `deny (IPv6)`
- `permit (MAC)`
- `deny (MAC)`
Example

switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005

48.12 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**

```plaintext
absolute start hh:mm day month year
no absolute start
absolute end hh:mm day month year
no absolute end
```

**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 (military format) and minutes (Range: 0–23, mm: 0–5)

- **day**—Day (by date) in the month. (Range: 1–31)

- **month**—Month (first three letters by name). (Range: Jan...Dec)

- **year**—Year (no abbreviation) (Range: 2000–2097)

**Default Configuration**

There is no absolute time when the time range is in effect.
Command Mode

Time-range Configuration mode

Example

switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005

48.13 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 day-of-the-week hh:mm to day-of-the-week hh:mm
no periodic day-of-the-week hh:mm to day-of-the-week hh:mm
periodic list hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]
no periodic list hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]
periodic list hh:mm to hh:mm all
no periodic list all hh:mm to hh:mm all

Parameters

- **day-of-the-week**—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). Possible values are: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.

- **hh:mm**—The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)
• list day-of-the-week1—Specifies a list of days that the time range is in effect.

Default Configuration
There is no periodic time when the time range is in effect.

Command Mode
Time-range Configuration mode

User Guidelines
The second occurrence of the day can be at the following week, e.g. Thursday–Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be on the following day, e.g. “22:00–2:00”.

Example

switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic Monday 12:00 to Wednesday 12:00

48.14 show time-range
Use the show time-range EXEC command to display the time range configuration.

Syntax
show time-range time-range-name

Parameters
time-range-name—Specifies the name of an existing time range.

Command Mode
EXEC mode

Example

switchxxxxxx# show time-range
http-allowed
absolute start 12:00 1 jan 2005
absolute end 12:00 31 dec 2005
periodic monday 8:00 to friday 20:00

48.15 show access-lists

Use the show access-lists Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

Syntax

show access-lists [name]
show access-lists time-range-active [name]

Parameters

- **name**—Specifies the name of the ACL.
- **time-range-active**—Shows only the Access Control Entries (ACEs) whose time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

Example

switchxxxxxx#show access-lists
Standard IP access list 1
deny any any
Standard IP access list 2
deny 192.168.0.0/24
permit any any
Standard IP access list 3
deny 192.168.0.1 10.0.0.0/8
permit any any
Standard IP access list ACL1
permit 192.168.0.0/16 10.1.1.1

Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any time-range weekdays

switchxxxxxx# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any

Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays

switchxxxxxx# show access-lists ACL1
Standard IP access list ACL1
permit 0.0.0.0
permit 192.168.0.2, wildcard bits 0.0.0.255

Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any

48.16 show interfaces access-lists

Use the show interfaces access-lists Privileged EXEC mode command to display access lists (ACLs) applied on interfaces.

Syntax

show interfaces access-lists [interface-id]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN.
Command Mode

Privileged EXEC mode

Example

switchxxxxxx# # show interfaces access-lists

<table>
<thead>
<tr>
<th>Interface</th>
<th>Ingress ACL</th>
<th>Egress ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>ACL1</td>
<td>ACL2</td>
</tr>
<tr>
<td>gi2</td>
<td>ACL3</td>
<td></td>
</tr>
<tr>
<td>gi3</td>
<td>blockcdp, blockvtp</td>
<td></td>
</tr>
</tbody>
</table>
Quality of Service (QoS) Commands

49.1 qos

Use the `qos` Global Configuration mode command to enable QoS on the device and set its mode. Use the `no` form of this command to disable QoS on the device.

Syntax

`qos [basic | advanced [ports-not-trusted | ports-trusted]]`

`no qos`

Parameters

- **basic**—QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.

- **advanced**—Specifies the QoS advanced mode, which enables the full range of QoS configuration.

- **ports-not-trusted**—Relevant for advanced mode only. Indicates that 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**—Relevant for advanced mode only. Indicates that 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 device.

```
switchxxxxxx(config)# qos
```

Example 2 - The following example enables QoS advanced mode on the device with the `ports-not-trusted` option.

```
switchxxxxxx(config)# qos advanced
```

### 49.2 qos advanced-mode trust

Use the `qos advanced-mode trust` Global Configuration command to configure the trust mode in advanced mode. Use the `no` form of this command to return to default.

**Syntax**

```
qos advanced-mode trust {cos | dscp | cos-dscp}
```

```
no qos advanced-mode trust
```

**Parameters**

- **cos**—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- **dscp**—Classifies ingress packets with the packet DSCP values.
- **cos-dscp**—Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.

**Default Configuration**

```
cos-dscp
```

**Command Mode**

Global Configuration

**User Guidelines**

The configuration is relevant for 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 by any QoS action or classified to the QoS action trust.

**Example**

The following example sets `cos` as the trust mode for QoS on the device.

```
switchxxxxxx(config)# qos advanced-mode trust cos
```

### 49.3 `show qos`

Use the `show qos` EXEC mode command to display the QoS information for the device. The trust mode is displayed for the QoS basic mode.

**Syntax**

```
show qos
```

**Parameters**

N/A

**Default Configuration**

Disabled Command Mode

**Command Mode**

EXEC mode

**User Guidelines**

Trust mode is displayed if QoS is enabled in basic mode.

**Examples**

**Example 1** - The following example displays QoS attributes when QoS is enabled in basic mode and the advanced mode is supported.

```
switchxxxxxx# show qos
```
Qos: basic
Basic trust: dscp

Example 2 - The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is not supported.

switchxxxxxx# show qos
Qos: disable
Trust: dscp

49.4 class-map

The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally-named service policy applied on a per-interface basis.

A class map consists of one or more ACLs (see ACL Commands). It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

Use the class-map Global Configuration mode command to create or modify a class map and enter the Class-map Configuration mode (only possible when QoS is in the advanced mode).

Use the no form of this command to delete a class map.

All class map commands are only available when QoS is in advanced mode.

Syntax

class-map class-map-name [match-all | match-any]

no class-map class-map-name

Parameters

- class-map-name—Specifies the class map name.
- match-all—Performs a logical AND of all the criteria of the ACLs belonging to this class map. All match criteria in this class map must be matched.
Quality of Service (QoS) Commands

- **match-any**—Performs a logical OR of the criteria of the ACLs belonging to this class map. Only a single match criteria in this class map must be matched.

**Default Configuration**

If neither **match-all** nor **match-any** is specified, the **match-all** parameter is selected by default.

**Command Mode**

Global Configuration mode

**User Guidelines**

The **class-map** enters 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 ACL and one MAC ACL. The classification is by first match, 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:

- **exit**: Exits the Class-map Configuration mode.
- **match**: Configures classification criteria.
- **no**: Removes 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-all
switchxxxxxx(config-cmap)#match access-group acl-name
```
49.5  **show class-map**

The **show class-map** EXEC mode command displays all class maps when QoS is in advanced mode.

**Syntax**

`show class-map [class-map-name]`

**Parameters**

`class-map-name`—Specifies the name of the class map to be displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays the class map for Class1.

```
switchxxxxxx# show class-map class1
Class Map match-any class1 (id4)
Match IP dscp 11 21
```

49.6  **match**

Use the **match** Class-map Configuration mode command to bind the ACLs that belong to the class-map being configured. Use the **no** form of this command to delete the ACLs.

This command is available only when the device is in QoS advanced mode.

**Syntax**

`match access-group acl-name`

`no match access-group acl-name`

**Parameters**

`acl-name`—Specifies the MAC or IP ACL name.
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 belong to the class map.

```
switchxxxxxx(config)# class-map class1
switchxxxxxx(config-cmap)# match access-group enterprise
```

49.7 policy-map

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/port-channels.

Use the policy-map Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the no form of this command to delete a policy map.

This command is only available when QoS is in advanced mode.

Syntax

```
policy-map policy-map-name
no policy-map policy-map-name
```

Parameters

```
policy-map-name—Specifies the policy map name.
```

Default Configuration

N/A

Command Mode

Global Configuration mode
User Guidelines

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 command 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/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)#
```

49.8 class

Use the **class** Policy-map Configuration mode command after the **policy-map** command to attach ACLs to a policy-map.

Use the **no** form of this command to detach a class map from a policy map.

This command is only available when QoS is in advanced mode.

Syntax

```
class class-map-name [access-group acl-name]
no class class-map-name
```

Parameters

- **class-map-name**—Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name.
- **access-group acl-name**—Specifies the name of an IP or MAC Access Control List (ACL).

**Default Configuration**
No class map is defined for the policy map.

**Command Mode**
Policy-map Configuration mode

**User Guidelines**
This is the same as creating a class map and then binding it to the policy map.

You can specify an existing class map in this command, or you can use the access-group parameter to create a new class map.

After the policy-map is defined, use the `service-policy` command to attach it to a port/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
switchxxxxxxx(config-pmap)# class class1 access-group enterprise
```

### 49.9 show policy-map

Use the `show policy-map` EXEC mode command to display all policy maps or a specific policy map.

This command is only available when QoS is in advanced mode.

**Syntax**

```
show policy-map [policy-map-name]
```

**Parameters**

- `policy-map-name`—Specifies the policy map name.
**Default Configuration**

All policy-maps are displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays all policy maps.

```plaintext
switchxxxxxxx#  show policy-map
Policy Map policy1
 class class1
  set IP dscp 7
Policy Map policy2
 class class 2
  police 96000 4800 exceed-action drop
 class class3
  police 124000 96000 exceed-action policed-dscp-transmit
```

### 49.10 trust

Use the `trust` Policy-map Class Configuration mode command to configure the trust state. This command is relevant only when QoS is in 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 the `no` form of this command to return to the default trust state.

This command is only available when QoS is in advanced mode.

**Syntax**

```plaintext
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

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 the incoming traffic.

The type of trust is determined in qos advanced-mode trust.

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 cl
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map pl
switchxxxxxx(config-pmap)# class cl
Quality of Service (QoS) Commands

49.11 set

Use the set Policy-map Class Configuration mode command to select the value that QoS uses as the DSCP value, the egress queue or to set user priority values.

This command is only available when QoS is in advanced mode.

Syntax

```
set {dscp new-dscp | queue queue-id | cos new-cos}
```

no set

Parameters

- **dscp new-dscp**—Specifies the new DSCP value for the classified traffic. (Range: 0–63)
- **queue queue-id**—Specifies the egress queue. (Range: 1-4)
- **cos new-cos**—Specifies the new user priority to be marked in the packet. (Range: 0–7)

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 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.

```
switchxxxxxxx(config)# ip access-list extended ip1
switchxxxxxxx(config-mac-al)# permit ip any any
switchxxxxxxx(config-mac-al)# exit
```
49.12 police

Use the police Policy-map Class Configuration mode command to define the policer for classified traffic. This defines another group of actions for the policy map (per class map).

This command is used after the policy-map and class commands.

Use the no form of this command to remove a policer.

This command is only available when QoS is in advanced mode.

Syntax

```
police committed-rate-kbps committed-burst-byte [exceed-action {drop | policed-dscp-transmit}]
```

no police

Parameters

- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (bps). Range: 100–10000000

- **committed-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)

- **exceed-action [drop | policed-dscp-transmit]**—Specifies the action taken when the rate is exceeded. The possible values are:
  - drop—Drops the packet.
  - policed-dscp-transmit—Remarks the packet DSCP, according to the policed-DSCP map as configured by the qos map policed-dscp Global Configuration mode command.
**Quality of Service (QoS) Commands**

**Default Usage**
N/A

**Command Mode**
Policy-map Class Configuration mode

**User Guidelines**
This command only exists in when the device is in Layer 2 mode.
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 a policer for classified traffic. When the traffic rate exceeds 124,000 kbps and the normal burst size exceeds 9600 bytes, 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 9600 exceed-action drop
```

**49.13 service-policy**
Use the `service-policy` Interface Configuration (Ethernet, Port-channel) mode command to bind a policy map to a port/port-channel. Use the `no` form of this command to detach a policy map from an interface.

This command is only available in QoS advanced mode.

**Syntax**
```
service-policy input policy-map-name default-action [permit-any | deny-any]
no service-policy input
```

**Parameters**
- `policy-map-name`—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)
- **deny-any**—Deny all the packets (which were ingress of the port) that do not meet the rules in a policy.

- **permit-any**—Forward all the packets (which were ingress of the port) that do not meet the rules in a policy.

**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)# service-policy input policy1 permit-any
```

### 49.14  qos aggregate-policer

Use the `qos aggregate-policer` Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the `no` form of this command to remove an existing aggregate policer.

This command is only available when QoS is in advanced mode.

**Syntax**

```
qos aggregate-policer aggregate-policer-name committed-rate-kbps excess-burst-byte [exceed-action {drop | policed-dscp-transmit}]
```

```
no qos aggregate-policer aggregate-policer-name
```

**Parameters**

- **aggregate-policer-name**—Specifies the aggregate policer name.

- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3–57982058)

- **excess-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
• **exceed-action** \{drop | policed-dscp-transmit\}—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP.

**Default Configuration**
No aggregate policer is defined.

**Command Mode**
Global Configuration mode

**User Guidelines**
This command only exists when the device is in Layer 2.

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, the 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 or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600
exceed-action drop
```
49.15  **show qos aggregate-policer**

Use the **show qos aggregate-policer** EXEC mode command to display aggregate policers.

This command is only available in QoS advanced mode.

**Syntax**

```
show qos aggregate-policer [aggregate-policer-name]
```

**Parameters**

*aggregate-policer-name*—Specifies the aggregate policer name.

**Default Configuration**

All policers are displayed.

**Command Mode**

EXEC mode

**Example**

The following example displays the parameters of the aggregate policer called Policer1.

```
switchxxxxxx#  show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

49.16  **police aggregate**

Use the **police aggregate** Policy-map Class Configuration mode command to apply an aggregate policer to multiple class maps within the same policy map. Use the no form of this command to remove an existing aggregate policer from a policy map.

This command is only available in QoS advanced mode.

**Syntax**

```
police aggregate aggregate-policer-name
```
no police aggregate aggregate-policer-name

Parameters
aggregate-policer-name—Specifies 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 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 9600
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
```

49.17 wrr-queue cos-map

Use the wrr-queue cos-map Global Configuration mode command to map Class of Service (CoS) values to a specific egress queue. Use the no form of this command to restore the default configuration.
Syntax

```
wrr-queue cos-map queue-id cos0... cos7
no wrr-queue cos-map [queue-id]
```

Parameters

- `queue-id`—Specifies the queue number to which the CoS values are mapped.
- `cos0... cos7`—Specifies up to 8 CoS values to map to the specified queue number. (Range: 0–7)

Default Configuration

The default CoS value mapping to 4 queues is as follows:

- CoS value 0 is mapped to queue 1.
- CoS value 1 is mapped to queue 1.
- CoS value 2 is mapped to queue 2.
- CoS value 3 is mapped to queue 3.
- CoS value 4 is mapped to queue 3.
- CoS value 5 is mapped to queue 4.
- CoS value 6 is mapped to queue 4.
- CoS value 7 is mapped to queue 4.

Command Mode

Global Configuration mode

User Guidelines

Use this command to distribute traffic to different queues.

Example

The following example maps CoS value 4 and 6 to queue 2.

```
switchxxxxxx(config)# wrr-queue cos-map 2 4 6
```
49.18  wrr-queue bandwidth

Use the wrr-queue bandwidth global Configuration command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the no form of this command to restore the default configuration.

Syntax

wrr-queue bandwidth weight1 weight2... weighting
no wrr-queue bandwidth

Parameters

weight1 weight1... weighting the ratio of bandwidth assigned by the WRR packet scheduler to the packet queues. See explanation in the User Guidelines. Separate each value by a space. (Range for each weight: 0–255)

Default Configuration

wrr is disabled by default. The default wrr weight is ‘1’ for all queues.

Command Mode

Global Configuration mode

User Guidelines

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. It is not recommended to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

An expedite 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
The following assigns WRR values to the queues.

```
switchxxxxxx(config)# wrr-queue bandwidth 6 6 6 6
```

### 49.19 priority-queue out num-of-queues

An expedite queue is a strict priority queue, which is serviced until empty before the other lower priority queues are serviced.

Use the `priority-queue out num-of-queues` Global Configuration mode command to configure the number of expedite queues. Use the `no` form of this command to restore the default configuration.

**Syntax**

```plaintext
priority-queue out num-of-queues number-of-queues
no priority-queue out num-of-queues
```

**Parameters**

- `number-of-queues`—Specifies the number of expedite (strict priority) queues. Expedite queues are assigned to the queues with the higher indexes. (Range: 0–4).
  - There must be either 0 wrr queues or more than one.
  - If `number-of-queues` = 0, all queues are assured forwarding (according to wrr weights) If the `number-of-queues` = 4, all queues are expedited (strict priority queues).

**Default Configuration**

All queues are expedite queues.

**Command Mode**

Global Configuration mode

**User Guidelines**

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
```

### 49.20 traffic-shape

The egress port shaper controls the traffic transmit rate (Tx rate) on a port.

Use the `traffic-shape` Interface Configuration mode command to configure the egress port shaper. Use the `no` form of this command to disable the shaper.

Syntax

```
traffic-shape committed-rate [committed-burst]
```

```
no traffic-shape
```

Parameters

- **committed-rate**—Specifies the maximum average traffic rate (CIR) in kbits per second (kbps). (Range: GE: 64kbps–maximum port speed; 10GE: 64Kbps–maximum port speed)

- **committed-burst**—Specifies the maximum permitted excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example sets a traffic shaper on `gi5` on queue 1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.
Quality of Service (QoS) Commands

49.21 traffic-shape queue

The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on a port.

Use the **traffic-shape queue** Interface Configuration mode command to configure the egress queue shaper. Use the **no** form of this command to disable the shaper.

**Syntax**

```
traffic-shape queue queue-id committed-rate [committed-burst]

no traffic-shape queue queue-id
```

**Parameters**

- **queue-id**—Specifies the queue number to which the shaper is assigned. (Range: 1-4)
- **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)
- **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

**Default Configuration**

The shaper is disabled.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**Example**

The following example sets a shaper on queue 1 on gi5 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# traffic-shape 1 124000 9600
```
49.22 rate-limit (Ethernet)

Use the `rate-limit` Interface Configuration mode command to limit the incoming traffic rate on a port. Use the `no` form of this command to disable the rate limit.

**Syntax**

```
rate-limit committed-rate-kbps [burst committed-burst-bytes]
no rate-limit
```

**Parameters**

- `committed-rate-kbps`—Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 100–max port speed.
- `burst committed-burst-bytes`—The burst size in bytes (3000–19173960). If unspecified, defaults to 128K.

**Default Configuration**

Rate limiting is disabled.

Committed-burst-bytes is 128K.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

Storm control and rate-limit (of Unicast packets) cannot be enabled simultaneously on the same port.

**Example**

The following example limits the incoming traffic rate on gi5 to 150,000 kbps.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# rate-limit 150000
```
49.23 rate-limit (VLAN)

Use the Layer 2 rate-limit (VLAN) Global Configuration mode command to limit the incoming traffic rate for a VLAN. Use the no form of this command to disable the rate limit.

Syntax

rate-limit vlan-id committed-rate committed-burst

no rate-limit vlan

Parameters

- vlan-id—Specifies the VLAN ID.
- committed-rate—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3-57982058)
- committed-burst—Specifies the maximum burst size (CBS) in bytes. (Range: 3000-19173960)

Default Configuration

Rate limiting is disabled.

Committed-burst-bytes is 128K.

Command Mode

Global Configuration mode

User Guidelines

Traffic policing in a policy map takes precedence over 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.

This command does not work in Layer 3 mode. It does not work in conjunction with IP Source Guard.

Example

The following example limits the rate on VLAN 11 to 150000 kbps or the normal burst size to 9600 bytes.
49.24 qos wrr-queue wrtd

Use the qos wrr-queue wrtd Global Configuration mode command to enable Weighted Random Tail Drop (WRTD). Use the no form of this command to disable WRTD.

Syntax
qos wrr-queue wrtd
no qos wrr-queue wrtd

Parameters
N/A

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
The command is effective after reset.

Example
switchxxxxxx(config)# qos wrr-queue wrtd
This setting will take effect only after copying running configuration to startup configuration and resetting the device
switchxxxxxx(config) #

49.25 show qos wrr-queue wrtd

Use the show qos wrr-queue wrtd Exec mode command to display the Weighted Random Tail Drop (WRTD) configuration.
Quality of Service (QoS) Commands

49.26 show qos interface

Use the show qos interface EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

show qos interface [buffers | queueing | policers | shapers | rate-limit] [interface-id]

Parameters

- **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the 4 queues.
- **queueing**—Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **policers**—Displays all the policers configured for this interface, their settings, and the number of policers currently unused (on a VLAN).
- **shapers**—Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **rate-limit**—Displays the rate-limit configuration.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

**Default Configuration**

N/A

**Command Mode**

EXEC mode

**User Guidelines**

If no parameter is specified with the `show qos interface` command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP-map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

**Examples**

**Example 1** - This is an example of the output from the `show qos interface queueing` command for 4 queues

```
witchxxxxxx#  show qos interface queueing gi1
Ethernet gi1

wrr bandwidth weights and EF priority:
  qid-weights      Ef - Priority
  1 - N/A          ena- 1
  2 - N/A          ena- 2
  3 - N/A          ena- 3
  4 - N/A          ena- 4

Cos-queue map:
  cos-qid
  0 - 1
  1 - 1
  2 - 2
  3 - 3
  4 - 3
```
Example 2 - This is an example of the output from the show qos interface shapers command

Ethernet gi1
Port shaper: disable
Committed rate: N/A
Committed burst: N/A

<table>
<thead>
<tr>
<th>Target</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>qid</td>
<td>Status</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>disable</td>
</tr>
<tr>
<td>2</td>
<td>disable</td>
</tr>
<tr>
<td>3</td>
<td>disable</td>
</tr>
<tr>
<td>4</td>
<td>disable</td>
</tr>
</tbody>
</table>
Example - 3 This is an example of the output from the `show qos interface policer` command.

```plaintext
switchxxxxxx# show qos interface policer gi1
Ethernet gi1
Class map: A
Policer type: aggregate
Committed rate: 192000 bps
Committed burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Committed rate: 192000 bps
Committed burst: 9600 bytes
Exceed-action: drop
Class map: C
Policer type: none
Committed rate: N/A
Committed burst: N/A
Exceed-action: N/A
```

Example 4 - This is an example of the output from the `show qos interface rate-limit` command.

```plaintext
switchxxxxxx# show qos interface rate-limit gi1
Port rate-limit [kbps] Burst [Bytes]
----- ------------------ ---------------
gi1 1000 512K
```

49.27 `wrr-queue`

Use the `wrr-queue` Global Configuration mode command to enable the tail-drop mechanism on an egress queue. Use the `no` form of this command to disable the tail-drop mechanism on an egress queue.

**Syntax**

- `wrr-queue tail-drop`
- `no wrr-queue`
Parameters

tail-drop— Specifies the tail-drop mechanism.

Default Configuration

The tail-drop mechanism on an egress queue is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command can only be used if Advanced mode is enabled.

Example

The following example enables the tail-drop mechanism on an egress queue.

```
switchxxxxxx(config)# wrr-queue tail-drop
```

### 49.28 qos wrr-queue threshold

Use the `qos wrr-queue threshold` Global Configuration mode command to assign queue thresholds globally. Use the `no` form of this command to restore the default configuration.

This command is only available in QoS advanced mode.

Syntax

```
qos wrr-queue threshold gigabitethernet queue-id thresholdPercentage
no qos wrr-queue threshold gigabitethernet queue-id
```

Parameters

- `gigabitethernet`— Specifies that the thresholds are to be applied to Gigabit Ethernet ports.
- `queue-id`— Specifies the queue number to which the tail-drop threshold is assigned.
• **threshold-percentage**—Specifies the queue threshold percentage value.

**Default Configuration**
The default threshold is 80 percent.

**Command Mode**
Global Configuration mode

**User Guidelines**
If the threshold is exceeded, packets with the corresponding Drop Precedence (DP) are dropped until the threshold is no longer exceeded.

**Example**
The following example assigns a threshold of 80 percent to WRR queue 1.

```
switchxxxxxx(config)# qos wrr-queue threshold gigabitethernet 1 80
```

### 49.29 qos map policed-dscp

Use the *qos map policed-dscp* Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the *no* form of this command to restore the default configuration.

This command is only available in QoS advanced mode.

**Syntax**

```
qos map policed-dscp dscp-list to dscp-mark-down
```

```
no qos map policed-dscp [dscp-list]
```

**Parameters**

- **dscp-list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)

- **dscp-mark-down**—Specifies the DSCP value to mark down. (Range: 0–63)

**Default Configuration**
The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.
Command Mode
Global Configuration mode.

User Guidelines
The original DSCP value and policed-DSCP value must be mapped to the same queue in order to prevent reordering.

Example
The following example marks incoming DSCP value 3 as DSCP value 5 on the policed-DSCP map.

```
switchxxxxxx(config)# qos map policed-dscp 3 to 5
```

49.30 qos map dscp-queue

Use the `qos map dscp-queue` Global Configuration mode command to configure the DSCP to CoS map. Use the `no` form of this command to restore the default configuration.

Syntax
```
qos map dscp-queue dscp-list to queue-id
no qos map dscp-queue [dscp-list]
```

Parameters

- `dscp-list`—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- `queue-id`—Specifies the queue number to which the DSCP values are mapped.

Default Configuration
The default map for 4 queues is as follows.

<table>
<thead>
<tr>
<th>DSCP value</th>
<th>0-15</th>
<th>16-23</th>
<th>24-39, 48-63</th>
<th>40-47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue-ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration mode

Example
The following example maps DSCP values 33, 40 and 41 to queue 1.

```
switchxxxxxx(config)# qos map dscp-queue 33 40 41 to 1
```

49.31 qos map dscp-dp

Use the `qos map dscp-dp` Global Configuration mode command to map the DSCP values to Drop Precedence. Use the `no` form of this command to restore the default configuration.

This command is only available in QoS advanced mode.

Syntax
```
qos map dscp-dp dscp-list to dp
no qos map dscp-dp [dscp-list]
```

Parameters
- `dscp-list`—Specifies up to 8 DSCP values, with values separated by a space. (Range: 0–63)
- `dp`—Specifies the Drop Precedence value to which the DSCP values are mapped. (Values: 0,2) where 2 is the highest Drop Precedence).

Default Configuration
All the DSCPs are mapped to Drop Precedence 0.

Command Mode
Global Configuration mode.

Example
The following example maps DSCP values 25, 27 and 29 to Drop Precedence 2.

```
switchxxxxxx(config)# qos map dscp-dp 25 27 29 to 2
```
49.32 qos trust (Global)

Use the `qos trust` Global Configuration mode command to configure the system to the basic mode and trust state. Use the `no` form of this command to return to the default configuration.

Syntax

```
qos trust {cos | dscp}
no qos trust
```

Parameters

- `cos`— Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- `dscp`— Specifies that ingress packets are classified with packet DSCP values.

Default Configuration

DSCP is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

This command can be used only in QoS basic mode.

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 system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.
For an inter-QoS domain boundary, configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different in the QoS domains.

Example
The following example configures the system to the DSCP trust state.

```bash
switchxxxxxx(config)# qos trust dscp
```

### 49.33 qos trust (Interface)

Use the `qos trust` Interface Configuration (Ethernet, Port-channel) mode command to enable port trust state while the system is in the basic QoS mode. Use the `no` form of this command to disable the trust state on each port.

**Syntax**

```bash
qos trust
no qos trust
```

**Parameters**

N/A

**Default Configuration**

Each port is enabled while the system is in basic mode.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**Example**

The following example configures `gi 15` to the default trust state.

```bash
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# qos trust
```
49.34  qos cos

Use the `qos cos` Interface Configuration (Ethernet, Port-channel) mode command to define the default CoS value of a port. Use the `no` form of this command to restore the default configuration.

**Syntax**

```
qos cos default-cos
no qos cos
```

**Parameters**

- `default-cos`—Specifies the default CoS value (VPT value) of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–7)

**Default Configuration**

The default CoS value of a port is 0.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

Use the default CoS value to assign a CoS value to all untagged packets entering the interface.

**Example**

The following example defines the port `gi5` default CoS value as 3.

```
switchxxxxxx(config)# interface gi5
switchxxxxxx(config-if)# qos cos 3
```

49.35  qos dscp-mutation

Use the `qos dscp-mutation` Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the `no` form of this command to restore the trusted port with no DSCP mutation.
Quality of Service (QoS) Commands

Syntax

qos dscp-mutation
no qos dscp-mutation

Parameters

N/A

Default Configuration

N/A

Command Mode

Global Configuration mode.

User Guidelines

Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port.

Global trust mode must be DSCP or CoS-DSCP. In advanced CoS mode, ports must be trusted.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
switchxxxxxx(config)# qos dscp-mutation
```

49.36  qos map dscp-mutation

Use the `qos map dscp-mutation` Global Configuration mode command to configure the DSCP to DSCP Mutation table. Use the `no` form of this command to restore the default configuration.
Quality of Service (QoS) Commands

49.37  **show qos map**

Use the `show qos map` EXEC mode command to display the various types of QoS mapping.

**Syntax**

```
show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]
```

**Example**

Use the `show qos map` command to display the various types of QoS mapping.

```
switchxxxxxx(config)# show qos map
```

---

**Syntax**

```
qos map dscp-mutation in-dscp to out-dscp
no qos map dscp-mutation [in-dscp]
```

**Parameters**

- **in-dscp**—Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- **out-dscp**—Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)

**Default Configuration**

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

**Command Mode**

Global Configuration mode.

**User Guidelines**

This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

**Example**

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
switchxxxxxx(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```
Parameters

- **dscp-queue**—Displays the DSCP to queue map.
- **dscp-dp**—Displays the DSCP to Drop Precedence map.
- **policed-dscp**—Displays the DSCP to DSCP remark table.
- **dscp-mutation**—Displays the DSCP-DSCP mutation table.

Default Configuration

Display all maps.

Command Mode

EXEC mode

Example

The following example displays the QoS mapping information:

Dscp-queue map:

```
 d1 : d2 0 1 2 3 4 5 6 7 8 9
    ------------------------------
  0 :   01 01 01 01 01 01 01 01 01 01
  1 :   01 01 01 01 01 01 02 02 02 02
  2 :   02 02 02 02 03 03 03 03 03 03
  3 :   03 03 03 03 03 03 03 03 03 03
  4 :   04 04 04 04 04 04 04 04 03 03
  5 :   03 03 03 03 03 03 03 03 03 03
  6 :   03 03 03 03
```

49.38 clear qos statistics

Use the `clear qos statistics` EXEC mode command to clear the QoS statistics counters.

Syntax

`clear qos statistics`
Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example clears the QoS statistics counters.

```
switchxxxxxx# clear qos statistics
```

### 49.39 qos statistics policer

Use the `qos statistics policer` Interface Configuration (Ethernet, Port-channel) mode command to enable counting in-profile and out-of-profile. Use the `no` form of this command to disable counting.

This command is relevant only when policers are defined.

**Syntax**

```
qos statistics policer policy-map-name class-map-name
no qos statistics policer policy-map-name class-map-name
```

**Parameters**

- **policy-map-name**—Specifies the policy map name.
- **class-map-name**—Specifies the class map name.

**Default Configuration**

Counting in-profile and out-of-profile is disabled.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode
Example
The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config-if)# qos statistics policer policy1 class1
```

### 49.40 qos statistics aggregate-policer

Use the **qos statistics aggregate-policer** Global Configuration mode command to enable counting in-profile and out-of-profile. Use the no form of this command to disable counting.

**Syntax**
```
qos statistics aggregate-policer aggregate-policer-name
no qos statistics aggregate-policer aggregate-policer-name
```

**Parameters**
- **aggregate-policer-name**—Specifies the aggregate policer name.

**Default Configuration**
Counting in-profile and out-of-profile is disabled.

**Command Mode**
Global Configuration mode

**Example**
The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config)# qos statistics aggregate-policer policer1
```

### 49.41 qos statistics queues

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues. Use the no form of this command to disable QoS statistics for output queues.
Quality of Service (QoS) Commands

Syntax

cos statistics queues set {queue | all} {dp | all} {interface | all}
no qos statistics queues set

Parameters

- set—Specifies the counter set number.
- interface—Specifies the Ethernet port.
- queue—Specifies the output queue number.
- dp—Specifies the drop precedence. The available values are: high, low.

Default Configuration

Set 1: All interfaces, all queues, high DP.
Set 2: All interfaces, all queues, low DP.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

If the queue parameter is all, traffic in cascading ports is also counted.

Example

The following example enables QoS statistics for output queues for counter set 1.

```
switchxxxxxx(config)# qos statistics queues 1 all all all
```

49.42 show qos statistics

Use the show qos statistics EXEC mode command to display Quality of Service statistical information.

Syntax

show qos statistics
Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

User Guidelines
Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Use the qos statistics queues Global Configuration mode command to enable QoS statistics for output queues.

Example
The following example displays Quality of Service statistical information.

```plaintext
switch# show qos statistics
Policers
--------
Interface  Policy map  Class Map  In-profile bytes  Out-of-profile bytes
----------  ---------  -------  --------------  ------------------
  gi1       Policy1    Class1  7564575          8759
  gi1       Policy1    Class2  8759             3214
  gi2       Policy1    Class1  746587458        23
  gi2       Policy1    Class2  5326
Aggregate Policers
-----------------
Name  In-profile bytes  Out-of-profile bytes
------  ------------------  ------------------
Policer1  7985687          121322
```
### Output Queues

<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue</th>
<th>DP</th>
<th>Total packets</th>
<th>TD packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi1</td>
<td>2</td>
<td>High</td>
<td>799921</td>
<td>1.2%</td>
</tr>
<tr>
<td>gi2</td>
<td>All</td>
<td>High</td>
<td>5387326</td>
<td>0.2%</td>
</tr>
</tbody>
</table>
Denial of Service (DoS) Commands

50.1 security-suite enable

Use the **security-suite enable** Global Configuration mode command to enable the security suite feature. This feature supports protection against various types of attacks.

When this command is used, hardware resources are reserved. These hardware resources are released when the **no security-suite enable** command is entered.

The security-suite feature can be enabled in one of the following ways:

- **Global-rules-only** - This enables the feature globally but per-interface features are not enabled.
- **All (no keyword)** - The feature is enabled globally and per-interface.

Use the **no** form of this command to disable the security suite feature.

When security-suite is enabled, you can specify the types of protection required. The following commands can be used:

- security-suite dos protect
- security-suite dos syn-attack
- security-suite deny martian-addresses
- security-suite deny syn
- security-suite deny icmp
- security-suite deny fragmented
- show security-suite configuration
- security-suite dos protect

**Syntax**

```
security-suite enable [global-rules-only]
```

```
no security-suite enable
```
Parameters

global-rules-only—Specifies that all the security suite commands are global commands only (they cannot be applied per-interface). This setting saves space in the Ternary Content Addressable Memory (TCAM). If this keyword is not used, security-suite commands can be used both globally on per-interface.

Default Configuration

The security suite feature is disabled.

If global-rules-only is not specified, the default is to enable security-suite globally and per interfaces.

Command Mode

Global Configuration mode

User Guidelines

MAC ACLs must be removed before the security-suite is enabled. The rules can be re-entered after the security-suite is enabled.

If ACLs or policy maps are assigned on interfaces, per interface security-suite rules cannot be enabled.

Examples

Example 1 - The following example enables the security suite feature and specifies that security suite commands are global commands only. When an attempt is made to configure security-suite on a port, it fails.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

Example 2 - The following example enables the security suite feature globally and on interfaces. The security-suite command succeeds on the port.

```
switchxxxxxx(config)# security-suite enable
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
```
Use the `security-suite dos protect` Global Configuration mode command to protect the system from specific well-known Denial of Service (DoS) attacks. There are three types of attacks against which protection can be supplied (see parameters below).

Use the `no` form of this command to disable DoS protection.

**Syntax**

```
security-suite dos protect {add attack | remove attack}
```

```
no security-suite dos protect
```

**Parameters**

- **add/remove attack**—Specifies the attack type to add/remove. To add an attack is to provide protection against it; to remove the attack is to remove protection.

The possible attack types are:

- **stacheldraht**—Discards TCP packets with source TCP port 16660.
- **invasor-trojan**—Discards TCP packets with destination TCP port 2140 and source TCP port 1024.
- **back-orifice-trojan**—Discards UDP packets with destination UDP port 31337 and source UDP port 1024.

**Default Configuration**

No protection is configured.

**Command Mode**

Global Configuration mode

**User Guidelines**

For this command to work, `security-suite enable` must be enabled globally.
Example
The following example protects the system from the Invasor Trojan DOS attack.

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

50.3 security-suite dos syn-attack

Use the `security-suite dos syn-attack` Interface Configuration mode command to rate limit Denial of Service (DoS) SYN attacks. This provides partial blocking of SYN packets (up to the rate that the user specifies).

Use the `no` form of this command to disable rate limiting.

Syntax

```
security-suite dos syn-attack syn-rate {any | ip-address} {mask | /prefix-length}
no security-suite dos syn-attack {any | ip-address} {mask | /prefix-length}
```

Parameters

- `syn-rate`—Specifies the maximum number of connections per second. (Range: 199–1000)
- `any | ip-address`—Specifies the destination IP address. Use `any` to specify all IP addresses.
- `mask`—Specifies the network mask of the destination IP address.
- `prefix-length`—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

No rate limit is configured.

If `ip-address` is unspecified, the default is 255.255.255.255

If `prefix-length` is unspecified, the default is 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode
User Guidelines

For this command to work, `security-suite enable` must be enabled both globally and for interfaces.

This command rate limits ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses.

SYN attack rate limiting is implemented after the security suite rules are applied to the packets. The ACL and QoS rules are not applied to those packets.

Since the hardware rate limiting counts bytes, it is assumed that the size of “SYN” packets is short.

Example

The following example attempts to rate limit DoS SYN attacks on a port. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

50.4 `security-suite deny martian-addresses`

Use the `security-suite deny martian-addresses` Global Configuration mode command to deny packets containing system-reserved IP addresses or user-defined IP addresses.

Syntax

```
security-suite deny martian-addresses [add {ip-address [mask | /prefix-length]} | remove {ip-address [mask | /prefix-length]}] (Add/remove user-specified IP addresses)

security-suite deny martian-addresses reserved [add | remove] (Add/remove system-reserved IP addresses, see tables below)

no security-suite deny martian-addresses (This command removes addresses reserved by `security-suite deny martian-addresses [add {ip-address [mask | /prefix-length]} | remove {ip-address [mask | /prefix-length]}], and removes all entries added by the user. The user can remove a specific entry by using `remove ip-address [mask | /prefix-length]` parameter.
```
There is no form of the `security-suite deny martian-addresses reserved [add | remove]` command. Use instead the `security-suite deny martian-addresses reserved remove` command to remove protection (and free up hardware resources).

**Parameters**

- **reserved add/remove**—Add or remove the table of reserved addresses below.
- **ip-address**—Adds/discards packets with the specified IP source or destination address.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).
- **reserved**—Discards packets with the source or destination IP address in the block of the reserved (Martian) IP addresses. See the User Guidelines for a list of reserved addresses.

**Default Configuration**

Martian addresses are allowed.

**Command Mode**

Global Configuration mode

**User Guidelines**

For this command to work, `security-suite enable` must be enabled globally.

`security-suite deny martian-addresses reserved` adds or removes the addresses in the following table:

<table>
<thead>
<tr>
<th>Address block</th>
<th>Present Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/8 (except when 0.0.0.0/32 is the source address)</td>
<td>Addresses in this block refer to source hosts on &quot;this&quot; network.</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>This block is assigned for use as the Internet host loopback address.</td>
</tr>
<tr>
<td>192.0.2.0/24</td>
<td>This block is assigned as “TEST-NET” for use in documentation and example code.</td>
</tr>
</tbody>
</table>
Denial of Service (DoS) Commands

### 50.5 security-suite deny syn

Use the `security-suite deny syn` Interface Configuration (Ethernet, Port-channel) mode command to block the creation of TCP connections from a specific interface. This a complete block of these connections.

Use the `no` form of this command to permit creation of TCP connections.

**Syntax**

```
security-suite deny syn [add {tcp-port | any} [ip-address | any] [mask | /prefix-length]] |
[remove {tcp-port | any} [ip-address | any] [mask | /prefix-length]]
```

**Parameters**

- `ip-address` | `any`—Specifies the destination IP address. Use `any` to specify all IP addresses.
- `mask`—Specifies the network mask of the destination IP address.
- `prefix-length`—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (`/`).

---

<table>
<thead>
<tr>
<th>Address block</th>
<th>Present Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0/4 as source</td>
<td>This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments.</td>
</tr>
<tr>
<td>240.0.0.0/4 (except when 255.255.255.255/32 is the destination address)</td>
<td>This block, formerly known as the Class E address space, is reserved.</td>
</tr>
</tbody>
</table>

Note that if the reserved addresses are included, individual reserved addresses cannot be removed.

**Example**

The following example discards all packets with a source or destination address in the block of the reserved IP addresses.

```
switchxxxxxx(config)# security-suite deny martian-addresses reserved add
```
Denial of Service (DoS) Commands

- **tcp-port | any**—Specifies the destination TCP port. The possible values are: http, ftp-control, ftp-data, ssh, telnet, smtp, dns, tftp, ntp, snmp or port number. Use any to specify all ports.

**Default Configuration**

Creation of TCP connections is allowed from all interfaces.

If the **mask** is not specified, it defaults to 255.255.255.255.

If the **prefix-length** is not specified, it defaults to 32.

**Command Mode**

Interface Configuration (Ethernet, Port-channel) mode

**User Guidelines**

For this command to work, **security-suite enable** must be enabled both globally and for interfaces.

The blocking of TCP connection creation from an interface is done by discarding ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses and destination TCP ports.

**Example**

The following example attempts to block the creation of TCP connections from an interface. It fails because security suite is enabled globally and not per interface.

```bash
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

---

### 50.6 **security-suite deny icmp**

Use the **security-suite deny icmp** Interface Configuration (Ethernet, Port-channel) mode command to discard ICMP echo requests from a specific interface (to prevent attackers from knowing that the device is on the network).

Use the **no** form of this command to permit echo requests.
Denial of Service (DoS) Commands

Syntax

security-suite deny icmp [add {ip-address | any} {mask | /prefix-length}] | [remove {ip-address | any} {mask | /prefix-length}]]

no security-suite deny icmp

Parameters

- ip-address | any—Specifies the destination IP address. Use any to specify all IP addresses.
- mask—Specifies the network mask of the IP address.
- prefix-length—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Echo requests are allowed from all interfaces.

If mask is not specified, it defaults to 255.255.255.255.

If prefix-length is not specified, it defaults to 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

For this command to work, security-suite enable must be enabled both globally and for interfaces.

This command discards ICMP packets with "ICMP type= Echo request" that ingress the specified interface.

Example

The following example attempts to discard echo requests from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.
50.7 security-suite deny fragmented

Use the security-suite deny fragmented Interface Configuration (Ethernet, Port-channel) mode command to discard IP fragmented packets from a specific interface.

Use the no form of this command to permit IP fragmented packets.

Syntax

security-suite deny fragmented [add {ip-address | any} {mask | /prefix-length}] | [remove {ip-address | any} {mask | /prefix-length}]

no security-suite deny fragmented

Parameters

- ip-address | any—Specifies the destination IP address. Use any to specify all IP addresses.
- mask— Specifies the network mask of the IP address.
- prefix-length—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Fragmented packets are allowed from all interfaces.

If mask is unspecified, the default is 255.255.255.255.

If prefix-length is unspecified, the default is 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

For this command to work, security-suite enable must be enabled both globally and for interfaces.

Example

The following example attempts to discard IP fragmented packets from an interface.
To perform this command, DoS Prevention must be enabled in the per-interface mode.

50.8 show security-suite configuration

Use the `show security-suite configuration` EXEC mode command to display the security-suite configuration.

Syntax

`show security-suite configuration`

Command Mode

EXEC mode

Example

The following example displays the security-suite configuration.

```
switchxxxxxx# show security-suite configuration
Security suite is enabled (Per interface rules are enabled).
Denial Of Service Protect: stacheldraht, invasor-trojan, back-office-trojan.
Denial Of Service SYN Attack
Interface       IP Address       SYN Rate (pps)  
--------------- -------------- -------------
gi1             176.16.23.0/24  100           
Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering
Interface       IP Address       TCP port  
--------------- -------------- ------------
gi2             176.16.23.0/24  FTP        
ICMP filtering
```

switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
50.9  **security-suite deny syn-fin**

Use the `security-suite deny syn-fin` Global Configuration mode command to drop all ingressing TCP packets in which both SYN and FIN flags are set.

Use the `no` form of this command to permit TCP packets in which both SYN and FIN are set.

**Syntax**

- `security-suite deny syn-fin`
- `no security-suite deny syn-fin`

**Parameters**

N/A

**Default Configuration**

Drop all ingressing TCP packets in which both SYN and FIN are set.

**Command Mode**

Global Configuration mode

**Example**

The following example blocks TCP packets in which both SYN and FIN flags are set.

```
switchxxxxxx(config)# security-suite deny syn-fin
```
50.10 security-suite syn protection mode

Use the `security-suite syn protection mode` Global Configuration mode command to set the TCP SYN protection mode.

Use the `no` form of this command to set the TCP SYN protection mode to default.

**Syntax**

```
security-suite syn protection mode {disabled | report | block}
no security-suite syn protection mode
```

**Parameters**

- `disabled`—The feature is disabled.
- `report`—The feature reports about TCP SYN traffic per port (including rate-limited SYSLOG messages when an attack is identified).
- `block`—the TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited SYSLOG message (one per minute) is generated.

**Default Configuration**

The default mode is `block`.

**Command Mode**

Global Configuration mode

**User Guidelines**

On ports in which an ACL is defined, this feature cannot block TCP SYN packets. If the protection mode is `block`, but SYN traffic cannot be blocked, a relevant SYSLOG message is created, e.g.: “port gi 1 is under TCP SYN attack. TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.”

**Examples**

**Example 1**—The following example sets the TCP SYN protection feature to report TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode report
```

...
01-Jan-2012 05:29:46: A TCP SYN Attack was identified on port gi1

Example 2—The following example sets the TCP SYN protection feature to block TCP SYN attack on ports if an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode block
```

... 01-Jan-2012 05:29:46: A TCP SYN Attack was identified on port gi1. TCP SYN traffic destined to the local system is automatically blocked for 100 seconds.

### 50.11 security-suite syn protection threshold

Use the `security-suite syn protection threshold` Global Configuration mode command to set the threshold for the SYN protection feature.

Use the `no` form of this command to set the threshold to its default value.

**Syntax**

```
security-suite syn protection threshold syn-packet-rate

no security-suite syn protection threshold
```

**Parameters**

- `syn-packet-rate`—Defines the rate from a specific port that triggers identification of a TCP SYN attack. (Range: 20-200 Packets Per Second (pps))

**Default Configuration**

The default threshold is 80 pps (packets per second).

**Command Mode**

Global Configuration mode

**Example**

The following example sets the TCP SYN protection threshold to 40 pps.

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```
50.12 security-suite syn protection recovery

Use the `security-suite syn protection recovery` Global Configuration mode command to set the time period for the SYN Protection feature to block an attacked interface.

Use the `no` form of this command to reset the time period to its default value.

**Syntax**

```
security-suite syn protection recovery timeout
no security-suite syn protection recovery
```

**Parameters**

- `timeout`—Defines 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 might become blocked again. (Range: 10-600 secs)

**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 TCP SYN period to 100 seconds.

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

50.13 show security-suite syn protection

Use the `show security-suite syn protection` EXEC mode command to display the security-suite configuration.
Syntax

`show security-suite syn protection interface-id`

Parameters

`interface-id`—Specifies an interface-ID. The interface-ID can be one of the following types: Ethernet port of Port-Channel. If this parameter is not provided, information is displayed for all interfaces.

Command Mode

EXEC mode

Example

The following example displays the TCP SYN protection feature configuration and current status on all interfaces. In this example, port 152 is attacked but since there is a user-ACL on this port, it cannot become blocked so its status is Reported and not Blocked and Reported.

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Current Status</th>
<th>Last Attack Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>151</td>
<td>Attacked</td>
<td>19:58:22.289 PDT Feb 19 2012</td>
<td>Blocked and Reported</td>
</tr>
<tr>
<td>152</td>
<td>Attacked</td>
<td>19:58:22.289 PDT Feb 19 2012</td>
<td>Reported</td>
</tr>
<tr>
<td>153</td>
<td>Attacked</td>
<td>19:58:22.289 PDT Feb 19 2012</td>
<td>Blocked and Reported</td>
</tr>
</tbody>
</table>
```
Router Resources Commands

51.1 system router resources

Use the `system router resources` command in Global Configuration mode to configure the system router resources.

Use the `no` form of this command to return to the default.

Syntax

```
system router resources [ip-entries max-number]
no system router resources
```

Parameters

- `ip-entries`—The maximum number of IPv4 entries.

Default Configuration

Product specific

Command Mode

Global configuration

User Guidelines

Use the `system router resources` command to enter new settings for routing entries. After entering the command, the current routing entries configuration will be displayed, and the user will be required to confirm saving the new setting to the startup-configuration and to reboot the system.

Data Validation:

- If the new settings exceed the maximum number of routing entries, the command is rejected and a message is displayed to the user.
- If the new settings are lower than the currently in-use routing entries, a confirmation message is displayed to the user (before the save confirmation message).

Use the `no system router resources` command to the default settings.
The following table displays the conversion between logical entities to HW entries:

**Examples**

**Example 1**

The following example defines the supported number of IPv4 and IPv6 routing entries. In the example, the configured router entries are less than the router entries which are currently in use. Using this configurations means that the system will not have enough resources for the running again in the existing network:

```
swxxxxxxx# system router resources ip-routes 128 ipv6-routes 32
```

The maximal number of IPv4 and IPv6 Routing Entries plus non-IP Entries is 2048.

<table>
<thead>
<tr>
<th>In-Use</th>
<th>Reserved (Current)</th>
<th>Reserved (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Entries</td>
<td>232</td>
<td>1024</td>
</tr>
<tr>
<td>Number of Routes</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Number of Neighbors</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Number of Interfaces</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

**Non-IP Entries:**

93% 400

The new configuration of route entries is less than the route entries which are currently in use by the system, do you want to continue (note that setting the new configuration of route entries requires saving the running-configuration file to startup-configuration file and rebooting the system)? (Y/N) [N] Y

**Example 2**

The following example defines the supported number of IPv4 routing entries.

```
swxxxxxxx# system router resources ip-routes 256
```

The maximal number of IPv4 and IPv6 Routing Entries plus non-IP Entries is 2048.

<table>
<thead>
<tr>
<th>In-Use</th>
<th>Reserved (Current)</th>
<th>Reserved (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Entries</td>
<td>.....</td>
<td>.....</td>
</tr>
</tbody>
</table>
IPv4 Entries                  232        1024               256
   Number of Routes           20
   Number of Neighbors        12
   Number of Interfaces      100
IPv6 Entries                  233        1024                32
   Number of Routes           20
   Number of Neighbors        12
   Number of Interfaces      100
   Number of On-Link Prefixes  1

Non-IP Entries:
   93%                   400

Setting the new configuration of route entries requires saving the
running-configuration file to startup-configuration file and rebooting the
system, do you want to continue? (Y/N) [N] Y

### 51.2 show system router resources

Use the **show system router resources** command in EXEC mode to display the
router resources.

**Syntax**

```
show system router resources
```

**Parameters**

This command has no arguments or keywords.

**Command Mode**

EXEC mode

**Examples**

**Example 1**—In the following example, the configured router entries are displayed:

```
switchxxxxxx#show system router resources
```

The maximal number of IPv4 and IPv6 Routing Entries plus Non-IP Entries is 2048.
<table>
<thead>
<tr>
<th></th>
<th>In-Use</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Entries</td>
<td>232</td>
<td>1024</td>
</tr>
<tr>
<td>Number of Routes</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Number of Neighbors</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Number of Interfaces</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>IPv6 Entries</td>
<td>233</td>
<td>1024</td>
</tr>
<tr>
<td>Number of Routes</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Number of Neighbors</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Number of Interfaces</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Non-IP Entries:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>93%</td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>
**DHCPv6 Commands**

### 52.1 ipv6 dhcp client stateless

Use the `ipv6 dhcp client stateless` command in Interface Configuration mode to enable DHCP for an IPv6 client process and to enable a request for stateless configuration through the interface on which the command is run.

Use the `no` form of this command to disable requests for stateless configuration.

**Syntax**

`ipv6 dhcp client stateless`

`no ipv6 dhcp client stateless`

**Parameters**

This command has no arguments or keywords.

**Default Configuration**

Information request is disabled on an interface.

**Command Mode**

Interface configuration

**User Guidelines**

Enabling this command starts the DHCPv6 client process if this process is not yet running and IPv6 interface is enabled on the interface.

This command enables the DHCPv6 Stateless service on the interface. The service allows to receive the some configuration from a DHCP server passed in the following options:

- **Option 23**: `OPTION_DNS_SERVERS` - List of DNS Servers IPv6 Addresses
- **Option 24**: `OPTION_DOMAIN_LIST` - Domain Search List
- **Option 31**: `OPTION_SNTP_SERVERS` - List of SNTP Servers IPv6 Addresses
- **Option 32:** OPTION_INFORMATION_REFRESH_TIME - Information Refresh Time Option
- **Option 41:** OPTION_NEW_POSIX_TIMEZONE - New Timezone Posix String
- **Option 59:** OPT_BOOTFILE_URL - Configuration Server URL
- **Option 60:** OPT_BOOTFILE_PARAM, the first parameter - Configuration File Path Name

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface.

**Example**

The following example enables the Stateless service:

```
interface vlan 100
  ipv6 dhcp client stateless
exit
```

## 52.2 clear ipv6 dhcp client

Use the `clear ipv6 dhcp client` command in Privileged EXEC mode to restart DHCP for an IPv6 client on an interface.

**Syntax**

```
clear ipv6 dhcp client interface-id
```

**Parameters**

`interface-id`—Interface identifier.

**Default Configuration**

N/A

**Command Mode**

Privileged EXEC
User Guidelines

This command restarts DHCP for an IPv6 client on a specified interface after first releasing and un-configuring previously-acquired prefixes and other configuration options (for example, DNS servers).

Example

The following example restarts the DHCP for IPv6 client on VLAN 100:

```
clear ipv6 dhcp client vlan 100
```

52.3 ipv6 dhcp client information refresh

Use the `ipv6 dhcp client information refresh` command in Interface Configuration mode to configure the refresh time for IPv6 client information on a specified interface if the DHCPv6 Server reply does not include the Information Refresh Time option.

Use the `no` form of this command to return to the default value of the refresh time.

Syntax

```
ipv6 dhcp client information refresh seconds / infinite
no ipv6 dhcp client information refresh
```

Parameters

- **seconds**—The refresh time, in seconds. The value cannot be less than the minimal acceptable refresh time configured by the `ipv6 dhcp client information refresh minimum` command. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFF).

- **infinite**—Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface configuration (config-if).
User Guidelines

This command specifies the information refresh time. If the server does not send an information refresh time option, the value configured by the command is used.

Use the infinite keyword to delete refresh, if the DHCP server does not send an information refresh time option.

Example

The following example configures an upper limit of 2 days:

```
interface vlan 100
  ipv6 dhcp client stateless
    ipv6 dhcp client information refresh 172800
exit
```

52.4 ipv6 dhcp client information refresh minimum

Use the ipv6 dhcp client information refresh minimum command in Interface Configuration mode to configure the minimum acceptable refresh time on the specified interface.

Use the no form of this command to remove the configured refresh time.

Syntax

```
ipv6 dhcp client information refresh minimum seconds/infinite
no ipv6 dhcp client information refresh minimum
```

Parameters

- **seconds**—The refresh time, in seconds. The minimum value that can be used is 600 seconds. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFF).

- **infinite**—Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).
Command Mode
Interface configuration (config-if).

User Guidelines
This command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

If you configure the infinite keyword, the client never refreshes the information.

Example
The following example configures an upper limit of 2 days:

```
interface vlan 100
  ipv6 dhcp client stateless
  ipv6 dhcp client information refresh minimum 172800
exit
```

52.5 ipv6 dhcp duid-en
Use the ipv6 dhcp duid-en command in Global Configuration mode to set the Vendor Based on Enterprise Number DHVPv6 Unique Identified (DUID-EN) format.

Use the no form of this command to return to the default value.

Syntax
ipv6 dhcp duid-en enterprise-number identifier
no ipv6 dhcp duid-en
Parameters

- **enterprise-number**—The vendor’s registered Private Enterprise number as maintained by IANA.

- **identifier**—The vendor-defined hex string (up to 64 hex characters). If the number of the character is not even, an ‘0’ is added at the right. Each 2 hex characters can be separated by a period or colon.

Default Configuration

DUID Based on Link-layer Address (DUID-LL) is used. The base MAC Address is used as a Link-layer Address.

Command Mode

Global Configuration.

User Guidelines

By default, the DHCPv6 uses the DUID Based on Link-layer Address (see RFC3315) with the Base MAC Address as a Link-layer Address.

Use this command to change the UDID format to the Vendor Based on Enterprise Number.

Examples

**Example 1**—The following sets the DIID-EN format:

```
ipv6 dhcp udid-en 9 0C084D303000912
```

**Example 2**—The following sets the DIID-EN format using colons as delimiter:

```
ipv6 dhcp udid-en 9 0C:C0:84:D3:03:00:09:12
```

52.6 ipv6 dhcp relay destination (Global)

Use the `ipv6 dhcp relay destination` command in global configuration mode to specify a globally-defined relay destination address to which client messages are forwarded.

Use the `no` form of this command to remove a relay destination address.
Syntax

```
ipv6 dhcp relay destination {ipv6-address [interface-id]} | interface-id
```

```
no ipv6 dhcp relay destination [ipv6-address [interface-id]] | interface-id
```

Parameters

- **ipv6-address**—Relay destination address. There are the following types of relay destination address:
  - Link-local unicast. A user must specify an output interface for this kind of address.
  - Global unicast IPv6 address. An output interface cannot be specified for this kind of address.

  This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.

  If the argument is not configured then the well know the link-local multicast address All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is defined.

- **interface-id**—Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected. If this argument is omitted then the Routing table is used.

Default Configuration

There is no globally defined relay destination.

Command Mode

Global configuration mode

User Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded. The address is used by all DHCPv6 relay running in the switch.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per the interface and globally.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays
messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination.

Use the no form of the command with the ipv6-address and interface-id arguments to remove only the given globally defined address with the given output interface.

Use the no form of the command with the ipv6-address argument to remove only the given globally defined address for all output interfaces.

The no form of the command without the arguments removes all the globally defined addresses.

Examples

Example 1—The following example sets the relay unicast link-local destination address per VLAN 200:

```
ipv6 dhcp relay destination FE80::1:2 vlan 200
```

Example 2—The following example sets the relay well known multicast link-local destination address per VLAN 200:

```
ipv6 dhcp relay destination vlan 200
```

Example 3—The following example sets the unicast global relay destination address:

```
ipv6 dhcp relay destination 3002::1:2
```

52.7 ipv6 dhcp relay destination (Interface)

Use the `ipv6 dhcp relay destination` command in Interface configuration mode to specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface.

Use the no form of this command to remove a relay destination on the interface or to delete an output interface for a destination.
DHCPv6 Commands

Syntax

ipv6 dhcp relay destination [ipv6-address [interface-id]] | interface-id
no ipv6 dhcp relay destination [ipv6-address [interface-id]] | interface-id

Parameters

- **ipv6-address**—Relay destination address. The following types of relay destination addresses exist:
  - Link-local unicast. A user must specify an output interface for this kind of address.
  - Global unicast IPv6 address. An output interface cannot be specified for this kind of address.

  This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.

  If the argument is not configured then the well-known link-local Multicast address All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is defined.

- **interface-id**—Specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Default Configuration

The relay function is disabled, and there is no relay destination on an interface.

Command Mode

Interface configuration (config-if)

User Guidelines

This command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface.

DHCPv6 Relay inserts the Interface-id option if an IPv6 global address is not defined on the interface on which the relay is running. The Interface-id field of the option is the interface name (a value of the ifName field of the ifTable) on which the relay is running.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per the interface and globally.
The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a Unicast address of a server or another relay agent, or it may be a Multicast address. There are two types of relay destination addresses:

- A link-local Unicast or Multicast IPv6 address, for which a user must specify an output interface.
- A global Unicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a Unicast or Multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a Multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local Multicast addresses are not acceptable as the relay destination.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface.

Use the `no` form of the command with arguments to remove a specific address.

Use the `no` form of the command without arguments to remove all the defined addresses and to disable the relay on the interface.

**Examples**

**Example 1**—The following example sets the relay Unicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
interface vlan 100
  ipv6 dhcp relay destination FE80::1:2 vlan 200
exit
```
Example 2—The following example sets the relay well known Multicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```plaintext
interface vlan 100
  ipv6 dhcp relay destination vlan 200
exit
```

Example 3—The following example sets the Unicast global relay destination address and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```plaintext
interface vlan 100
  ipv6 dhcp relay destination 3002::1:2
exit
```

Example 4. The following example enables the DHCPv6 relay on VLAN 100:

```plaintext
interface vlan 100
  ipv6 dhcp relay destination
exit
```

Example 5. The following example disables the DHCPv6 relay on VLAN 100:

```plaintext
interface vlan 100
  no ipv6 dhcp relay destination
exit
```

52.8 show ipv6 dhcp

Use the `show ipv6 dhcp` command in User EXEC or Privileged EXEC mode to display the Dynamic DHCP Unique Identifier (DUID) on a specified device. This information is relevant for DHCPv6 client and DHCPv6 relay.
Syntax
show ipv6 dhcp

Parameters
NA

Command Mode
User EXEC
Privileged EXEC

User Guidelines
This command uses the DUID, based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

Examples
Example 1—The following is sample output from this command when the switch’s UDID format is Vendor Based on Enterprise Number:

```
show ipv6 dhcp
The switch’s DHCPv6 unique identifier(DUID)is 0002000000090CC084D303000912
  Format: 2
  Enterprise Number: 9
  Identifier: 0CC084D303000912
```

Example 2—The following is sample output from this command when the switch’s UDID format is the vendor-based on a link-layer address:

```
show ipv6 dhcp
The switch’s DHCPv6 unique identifier(DUID)is 000300010024012607AA
  Format: 3
  Hardware type: 1
  MAC Address: 0024.0126.07AA
```
52.9 show ipv6 dhcp interface

Use the show ipv6 dhcp interface command in User EXEC or Privileged EXEC mode to display DHCP for IPv6 interface information.

Syntax

show ipv6 dhcp interface [interface-id]

Parameters

interface-id—Interface identifier.

Command Mode

User EXEC
Privileged EXEC

User Guidelines

If no interfaces are specified in the command, all interfaces on which DHCP for IPv6 (client or server) is enabled are displayed. If an interface is specified in the command, only information about the specified interface is displayed.

Examples

Example 1—The following is sample output from this command when only the Stateless service is enabled:

```
show ipv6 dhcp interface
  gi is in client mode
  DHCP Operational mode is enabled
  Stateless Service is enabled
  Reconfigure service is enabled
  Information Refresh Minimum Time: 600 seconds
  Information Refresh Time: 86400 seconds
  Received Information Refresh Time: 3600 seconds
  Remain Information Refresh Time: 411 seconds
  DHCP server:
    Address FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
```
Preference: 20
DNS Servers: 1001::1, 2001::10
DNS Domain Search List: company.com beta.org
SNTP Servers: 2004::1
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
Configuration Server: config.company.com
Configuration Path Name: qqq/config/aaa_config.dat
gi2 is in client mode
DHCP Operational mode is disabled (IPv6 is not enabled)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh Minimum Time: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
gi3 is in client mode
DHCP Operational mode is disabled (Interface status is DOWN)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh Minimum Time: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
gi4 is in relay mode
DHCP Operational mode is enabled
Relay source interface: VLAN 101
Relay destinations:
  FE80::250:A2FF:FEBF:A056 via gi10
gi5 is in client mode
DHCP Operational mode is disabled (Interface status is DOWN)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh Minimum Time: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
DHCP server:
  Address FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
Preference: 20
Received Information Refresh Time: 3600 seconds
DNS Servers: 1001::1, 2001::10
DNS Domain Search List: company.com beta.org
SNTP Servers: 2004::1
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
Configuration Server: config.company.com
Configuration Path Name: qqq/config/aaa_config.dat
DHCP Server Commands

53.1 ip dhcp server

Use the `ip dhcp server` Global Configuration mode command to enable the DHCP server features on the device.

Use the `no` form of this command to disable the DHCP server.

**Syntax**

```
ip dhcp server
no ip dhcp server
```

**Default Configuration**

The DHCP server is disabled.

**Command Mode**

Global Configuration mode

**Example**

The following example enables the DHCP server on the device:

```
Console(config)# ip dhcp server
```

53.2 ip dhcp pool host

Use the `ip dhcp pool host` Global Configuration mode command to configure a DHCP static address on a DHCP Server and enter the DHCP Pool Host Configuration mode.

Use the `no` form of this command to remove the address pool.

**Syntax**

```
ip dhcp pool host name
no ip dhcp pool host name
```

**Parameters**

`name`—Specifies the DHCP address pool name. It can be either a symbolic string (such as Engineering) or an integer (such as 8). (Length: 1–32 characters)
Default Configuration
DHCP hosts are not configured.

Command Mode
Global Configuration mode

User Guidelines
During execution of this command, the configuration mode changes to the DHCP Pool Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure host parameters, such as the IP subnet number and default router list.

Example
The following example configures station as the DHCP address pool:

```
Console(config)# ip dhcp pool host station

Console(config-dhcp)#
```

53.3 ip dhcp pool network

Use the `ip dhcp pool network` Global Configuration mode command to configure a DHCP address pool on a DHCP Server and enter DHCP Pool Configuration mode. Use the no form of this command to remove the address pool.

Syntax

```
ip dhcp pool network name
no ip dhcp pool network name
```

Parameters

`name`—Specifies the DHCP address pool name. It can be either a symbolic string (such as ‘engineering’) or an integer (such as 8). (Length: 1–32 characters)

Default Configuration
DHCP address pools are not configured.

Command Mode
Global Configuration mode

User Guidelines
During execution of this command, the configuration mode changes to DHCP Pool Network Configuration mode, which is identified by the (config-dhcp)# prompt. In
this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Example
The following example configures Pool1 as the DHCP address pool.

```
Console(config)# ip dhcp pool network Pool1
Console(config-dhcp)#
```

53 4  address (DHCP Host)

Use the address DHCP Pool Host Configuration mode command to manually bind an IP address to a DHCP client.

Use the no form of this command to remove the IP address binding to the client.

Syntax

```
address ip-address {mask | prefix-length} [client-identifier unique-identifier | hardware-address mac-address]
no address
```

Parameters

- **address**—Specifies the client IP address.
- **mask**—Specifies the client network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **unique-identifier**—Specifies the distinct client identification in dotted hexadecimal notation. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. For example, 01b70813.8811.66.
- **hardware-address**—Specifies the MAC address.

Default Configuration

No address are bound.
Command Mode

DHCP Pool Host Configuration mode

Example

The following example manually binds an IP address to a DHCP client.

```
Console(config-dhcp)# address 10.12.1.99 255.255.255.0 01b7.0813.8811.66
```

53.5 address (DHCP Network)

Use the address DHCP Pool Network Configuration mode command to configure the subnet number and mask for a DHCP address pool on a DHCP server. Use the no form of this command to remove the subnet number and mask.

Syntax

```
address [network-number | low low-address high high-address] {mask | prefix-length}
no address
```

Parameters

- network-number—Specifies the IP address of the DHCP address pool.
- mask—Specifies the pool network mask.
- prefix-length—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- low low-address—Specifies the first IP address to use in the address range.
- high high-address—Specifies the last IP address to use in the address range.

Default Configuration

DHCP address pools are not configured.

If the **low address** is not specified, it defaults to the first IP address in the network.

If the **high address** is not specified, it defaults to the last IP address in the network.
Command Mode
DHCP Pool Network Configuration mode

Example
The following example configures the subnet number and mask for a DHCP address pool on DHCP server.

```
Console(config-dhcp)# address 10.12.1.0 255.255.255.0

53.6 lease

Use the lease DHCP Pool Network Configuration mode command to configure the time duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client.

Use the no form of this command to restore the default value.

Syntax
lease {days [[hours] [minutes]] | infinite}
no lease

Parameters
- days—Specifies the number of days in the lease.
- hours—Specifies the number of hours in the lease. A days value must be supplied before configuring an hours value.
- minutes—Specifies the number of minutes in the lease. A days value and an hours value must be supplied before configuring a minutes value.
- infinite—Specifies that the duration of the lease is unlimited.

Default Configuration
The default lease duration is 1 day.

Command Mode
DHCP Pool Network Configuration mode

Examples
The following example shows a 1-day lease.
The following example shows a one-hour lease.

The following example shows a one-minute lease.

The following example shows an infinite (unlimited) lease.

53.7 client-name

Use the client-name DHCP Pool Host Configuration mode command to define the name of a DHCP client. The client name should not include the domain name.

Use the no form of this command to remove the client name.

Syntax
client-name name
no client-name

Parameters
name—Specifies the client name, using standard ASCII characters. The client name should not include the domain name. For example, the name Mars should not be specified as mars.yahoo.com. (Length: 1–32 characters)

Command Mode
DHCP Pool Host Configuration mode

Default Configuration
No client name is defined.

Example
The following example defines the string client1 as the client name.

Console(config-dhcp)# client-name client1
53.8 default-router

Use the `default-router` DHCP Pool Configuration mode command to configure the default router list for a DHCP client.

Use the `no` form of this command to remove the default router.

**Syntax**

```
default-router ip-address [ip-address2 ... ip-address8]
```

```
no default-router
```

**Parameters**

- `ip-address`: Specifies the IP address of a router. One IP address is required, although up to eight addresses can be specified in one command line.

**Command Mode**

- DHCP Pool Host Configuration mode
- DHCP Pool Network Configuration mode

**Default Configuration**

No default router is defined.

**User Guidelines**

The router IP address should be on the same subnet as the client subnet.

**Example**

The following example specifies 10.12.1.99 as the default router IP address.

```
Console(config-dhcp)# default-router 10.12.1.99
```

53.9 dns-server

Use the `dns-server` DHCP Pool Configuration mode command to configure the Domain Name System (DNS) IP servers available to a DHCP client.

Use the `no` form of this command to remove the DNS server list.

**Syntax**

```
dns-server ip-address [ip-address2 ... ip-address8]
```

```
no dns-server
```
**53.10 domain-name**

Use the `domain-name` DHCP Pool Configuration mode command to specify the domain name for a DHCP client.

Use the `no` form of this command to remove the domain name.

**Syntax**

```
domain-name domain
```

**Parameters**

domain—Specifies the DHCP client domain name string. (Length: 1–32 characters)

**Command Mode**

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

**Default Configuration**

No domain name is defined.
Example
The following example specifies yahoo.com as the DHCP client domain name string.

```
Console(config-dhcp)# domain-name yahoo.com
```

### 53.11 netbios-name-server

Use the **netbios-name-server** DHCP Pool Configuration mode command to configure the NetBIOS Windows Internet Naming Service (WINS) servers that are available to Microsoft DHCP clients.

Use the **no** form of this command to remove the NetBIOS name server.

**Syntax**

```
netbios-name-server ip-address
no netbios-name-server
```

**Parameters**

- `ip-address`—Specifies the NetBIOS WINS name server IP address.

**Command Mode**

- DHCP Pool Host Configuration mode
- DHCP Pool Network Configuration mode

**Default Configuration**

No bios server is defined.

**Example**

The following example specifies the IP address of a NetBIOS name server available to the DHCP client.

```
Console(config-dhcp)# netbios-name-server 10.12.1.90
```

### 53.12 netbios-node-type

Use the **netbios-node-type** DHCP Pool Configuration mode command to configure the NetBIOS node type for Microsoft DHCP clients.

Use the **no** form of this command to return to default.
Syntax
netbios-node-type {b-node /p-node /m-node /h-node}
no netbios-node-type

Parameters
- b-node—Specifies the Broadcast NetBIOS node type.
- p-node—Specifies the Peer-to-peer NetBIOS node type.
- m-node—Specifies the Mixed NetBIOS node type.
- h-node—Specifies the Hybrid NetBIOS node type.

Command Mode
DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Default Configuration
h-node (Hybrid NetBIOS node type).

Example
The following example specifies the client's NetBIOS type as mixed.

```
Console(config-dhcp)# netbios node-type m-node
```

53.13 next-server

Use the next-server DHCP Pool Configuration mode command to configure the next server (siaddr) in the boot process of a DHCP client. The client will connect, using SCP/TFTP, to this server in order to download the boot file.

Use the no form of this command to remove the boot server.

Syntax
next-server ip-address
no next-server

Parameters
- ip-address—Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
Default Configuration
If the `next-server` command is not used to configure a boot server list, the DHCP server uses inbound interface helper addresses as boot servers.

Command Mode
DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

Example
The following example specifies 10.12.1.99 as the IP address of the next server in the boot process.

```
Console(config-dhcp)# next-server 10.12.1.99
```

### 53.14 `next-server-name`

Use the `next-server-name` DHCP Pool Configuration mode command to configure the next server name (sname) in the boot process of a DHCP client. The client will connect, using SCP/TFTP, to this server in order to download the bootfile.

Use the `no` form of this command to remove the boot server name.

**Syntax**

```
next-server-name name
no next-server-name
```

**Parameters**

`name`—Specifies the name of the next server in the boot process. (Length: 1–64 characters)

**Command Mode**

DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

**Default Configuration**

No next server name is defined.

**Example**

The following example specifies `www.bootserver.com` as the name of the next server in the boot process of a DHCP client.

```
```
53.15  bootfile

Use the **bootfile** DHCP Pool Configuration mode command to specify the default boot image file name for a DHCP client.

Use the no form of this command to delete the boot image file name.

**Syntax**

```
bootfile filename
```

```
no bootfile
```

**Parameters**

- `filename`—Specifies the file name used as a boot image. (Length: 1–128 characters)

**Command Mode**

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

**Example**

The following example specifies boot_image_file as the default boot image file name for a DHCP client.

```
Console(config-dhcp)# bootfile boot_image_file
```

53.16  time-server

Use the **time-server** DHCP Pool Configuration mode command to specify the time server for a DHCP client.

Use the no form of this command to remove the time servers.

**Syntax**

```
time-server ip-address
```

```
no time-server
```

**Parameters**

- `ip-address`—Specifies the IP address of a time server.
**Command Mode**
DHCP Pool Host Configuration mode
DHCP Pool Network Configuration mode

**Default Configuration**
No time server name is defined.

**User Guidelines**
The time server's IP address should be on the same subnet as the client subnet.

**Example**
The following example specifies 10.12.1.99 as the time server IP address.

```
Console(config-dhcp)# time-server 10.12.1.99
```

### 53.17 option

Use the `option` DHCP Pool Configuration mode command to configure the DHCP server options.

Use the `no` form of this command to remove the options.

**Syntax**

```
option code {ascii ascii-string | hex hex-string | ip ip-address}
option ip-list code ip-address 1 [ip-address2 ...]
no option code
```

**Parameters**

- `code`—Specifies the DHCP option code.
- `ascii ascii-string`—Specifies an NVT ASCII character string. ASCII character strings, which contain white space, must be delimited by quotation marks.
- `hex hex-string`—Specifies dotted hexadecimal data: Each byte in hexadecimal character strings is two hexadecimal digits. Bytes are separated by a period or colon.
- `ip ip-address`—Specifies an IP address.
- `ip-list`—Specifies that a list of IP addresses immediately follows the option code.
- \texttt{ip-address1[ip-address2 ...]}—Specifies a list of one or more IP addresses.

**Command Mode**

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

**User Guidelines**

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the DHCP message options field. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, *Dynamic Host Configuration Protocol*.

For options in hexadecimal format, the string parameter should include all the bytes in the option value, including leading zeros.

**Examples**

**Example 1** - The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding. A value of 1 means enable IP forwarding. IP forwarding is enabled in the following example.

```
Console(config-dhcp)# option 19 hex 01
```

**Example 2** - The following example configures DHCP option 2, which specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). A value of 0xE10 in the following example indicates a location 1 hour east of the meridian.

```
Console(config-dhcp)# option 2 hex 00000E10
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example.

```
Console(config-dhcp)# option ip-list 72 172.16.3.252 172.16.3.253
```
53.18  ip dhcp excluded-address

Use the `ip dhcp excluded-address` Global Configuration mode command to specify the IP addresses that a DHCP server should not assign to DHCP clients. Use the `no` form of this command to remove the excluded IP addresses.

Syntax

```
ip dhcp excluded-address low-address [high-address]
no ip dhcp excluded-address low-address [high-address]
```

Parameters

- `low-address`—Specifies the excluded IP address, or first IP address in an excluded address range.
- `high-address`—Specifies the last IP address in the excluded address range.

Default Configuration

All IP pool addresses are assignable.

Command Mode

Global Configuration mode

User Guidelines

The DHCP server assumes that all pool addresses can be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Example

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199.

```
Console(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

53.19  clear ip dhcp binding

The `clear ip dhcp binding` Privileged EXEC mode command deletes the dynamic address binding from the DHCP server database.

Syntax

```
clear ip dhcp binding {address | *}
```
Parameters

- **address** — Specifies the binding address to delete from the DHCP database.
- * — Clears all automatic bindings.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

Typically, the address supplied denotes the client IP address. If the asterisk (*) character is specified as the address parameter, DHCP clears all dynamic bindings.

Use the **no ip dhcp pool** Global Configuration mode command to delete a manual binding.

**Example**

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Console# clear ip dhcp binding 10.12.1.99
```

### 53.20 show ip dhcp

The **show ip dhcp** EXEC mode command displays the DHCP configuration.

**Syntax**

```
show ip dhcp
```

**Command Mode**

EXEC mode

**Example**

The following example displays the DHCP configuration.

```
console# show ip dhcp
DHCP server is enabled.
DHCP ping packets is enabled with 2 retries and 500 milliseconds.
```
53.21  show ip dhcp excluded-addresses

The show ip dhcp excluded-addresses EXEC mode command displays the excluded addresses.

Syntax
show ip dhcp excluded-addresses

Command Mode
EXEC mode

Example
The following example displays the excluded addresses.

console# show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2
Excluded addresses:
10.1.1.212- 10.1.1.219, 10.1.2.212- 10.1.2.219

53.22  show ip dhcp pool host

The show ip dhcp pool host EXEC mode command displays the DHCP pool host configuration.

Syntax
show ip dhcp pool host [address | name]

Parameters
- address — Specifies the client IP address.
- name — Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode
EXEC mode

Example s
Example 1 - The following example displays configuration of all DHCP host pools:

console# show ip dhcp pool host
The number of host pools is 1

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Hardware Address</th>
<th>Client Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>station</td>
<td>172.16.1.11</td>
<td></td>
<td>01b7.0813.8811.66</td>
</tr>
</tbody>
</table>

Example 2 - The following example displays the DHCP pool host configuration with name station:

```console
console# show ip dhcp pool host station
```

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Hardware Address</th>
<th>Client Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>station</td>
<td>172.16.1.11</td>
<td></td>
<td>01b7.0813.8811.66</td>
</tr>
</tbody>
</table>

Mask: 255.255.0.0

Default router: 172.16.1.1

Client name: client1

DNS server: 10.12.1.99

Domain name: yahoo.com

NetBIOS name server: 10.12.1.90

NetBIOS node type: h-node

Next server: 10.12.1.99

Next-server-name: 10.12.1.100

Bootfile: Bootfile

Time server 10.12.1.99

Options:

<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>integer</td>
<td>3600</td>
</tr>
<tr>
<td>14</td>
<td>ascii</td>
<td>qq/aaaa/bbb.txt</td>
</tr>
<tr>
<td>19</td>
<td>boolean</td>
<td>false</td>
</tr>
<tr>
<td>21</td>
<td>ip</td>
<td>134.14.14.1</td>
</tr>
<tr>
<td>31</td>
<td>ip-list</td>
<td>1.1.1.1, 12.23.45.2</td>
</tr>
</tbody>
</table>
53.23  show ip dhcp pool network

The show ip dhcp pool network EXEC mode command displays the DHCP network configuration.

Syntax
show ip dhcp pool network [name]

Parameters
name — Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode
EXEC mode

Example
The following example displays configuration of all DHCP network pools:

Router> show ip dhcp pool network

The number of network pools is 2

Name Address range mask Lease
--------------------------------- ------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
finance 10.1.2.8-10.1.2.178 255.255.255.0 0d:12h:0m

Router> show ip dhcp pool network marketing

Name Address range mask Lease
--------------------------------- ------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m

Statistics:
All-range Available Free Pre-allocated Allocated Expired Declined
--------- ------- ----- ---------- ------- ------- ------- ------- -------
162 150 68 50 20 3 9

Default router: 10.1.1.1
Ping packets: enabled
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code  Value
---  ------------------
2     3600
14    qq/aaaa/bbb.txt
19    false
21    134.14.14.1
31    1.1.1.1, 12.23.45.2
47    02af00aa00

53.24 show ip dhcp binding

Use the show ip dhcp binding EXEC mode command to display the specific address binding or all the address bindings on the DHCP server.

Syntax
show ip dhcp binding [ip-address]

Parameters
ip-address — Specifies the IP address

Command Mode
EXEC mode

Examples
The following examples display the DHCP server binding address parameters.
Router> **show ip dhcp binding**

DHCP server enabled

The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware Address</th>
<th>Lease Expiration</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.16.1.11</td>
<td>00a0.9802.32de</td>
<td>Feb 01 1998</td>
<td>dynamic allocated</td>
<td></td>
</tr>
<tr>
<td>1.16.3.23</td>
<td>02c7.f801.0422</td>
<td>12:00AM</td>
<td>dynamic expired</td>
<td></td>
</tr>
<tr>
<td>1.16.3.24</td>
<td>02c7.f802.0422</td>
<td></td>
<td>dynamic declined</td>
<td></td>
</tr>
<tr>
<td>1.16.3.25</td>
<td>02c7.f803.0422</td>
<td></td>
<td>dynamic pre-allocated</td>
<td></td>
</tr>
<tr>
<td>1.16.3.26</td>
<td>02c7.f804.0422</td>
<td></td>
<td>dynamic declined</td>
<td></td>
</tr>
</tbody>
</table>

Router> **show ip dhcp binding**  1.16.1.11

DHCP server enabled

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware Address</th>
<th>Lease Expiration</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.16.1.11</td>
<td>00a0.9802.32de</td>
<td>Feb 01 1998</td>
<td>dynamic allocated</td>
<td></td>
</tr>
</tbody>
</table>

12:00 AM

Router> **show ip dhcp binding**  1.16.3.24

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware Address</th>
<th>Lease Expiration</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.16.3.24</td>
<td>02c7.f802.0422</td>
<td></td>
<td>dynamic declined</td>
<td></td>
</tr>
</tbody>
</table>
The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The host IP address as recorded on the DHCP server.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>The MAC address or client identifier of the host as recorded on the DHCP server.</td>
</tr>
<tr>
<td>Lease expiration</td>
<td>The lease expiration date of the host IP address.</td>
</tr>
<tr>
<td>Type</td>
<td>The manner in which the IP address was assigned to the host.</td>
</tr>
<tr>
<td>State</td>
<td>The IP Address state.</td>
</tr>
</tbody>
</table>

53.25 show ip dhcp server statistics

Use the `show ip dhcp server statistics` EXEC command to display DHCP server statistics.

**Syntax**

```
show ip dhcp server statistics
```

**Command Mode**

EXEC mode

**Example**

The following example displays DHCP server statistics

```
DHCP server enabled
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```
53.26 show ip dhcp allocated

Use the `show ip dhcp allocated` EXEC mode command to display the specific allocated address or all the allocated addresses on the DHCP server.

Syntax

```
show ip dhcp allocated [ip-address]
```

Parameters

`ip-address` — Specifies the IP address

Command Mode

EXEC mode

Example

The following example displays the DHCP server allocated IP addresses.

```
Router> show ip dhcp allocated
DHCP server enabled
The number of allocated entries is 3
IP Address   Hardware Address Lease Expiration      Type
----------   ---------------- --------------------  ---------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic
172.16.3.253 02c7.f800.0422   Infinite              Automatic
172.16.3.254 02c7.f800.0422   Infinite              Static
Router> show ip dhcp allocated 172.16.1.11
DHCP server enabled
The number of allocated entries is 2
IP Address   Hardware Address Lease Expiration      Type
----------   ---------------- --------------------  --------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic
Router> show ip dhcp allocated 172.16.3.254
DHCP server enabled
The number of allocated entries is 2
IP Address   Hardware Address Lease Expiration      Type
----------   ---------------- --------------------  --------
The following table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The host IP address as recorded on the DHCP server.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>The MAC address or client identifier of the host as recorded on the DHCP server.</td>
</tr>
<tr>
<td>Lease expiration</td>
<td>The lease expiration date of the host IP address.</td>
</tr>
<tr>
<td>Type</td>
<td>The manner in which the IP address was assigned to the host.</td>
</tr>
</tbody>
</table>

### 53.27 show ip dhcp declined

Use the `show ip dhcp declined` EXEC command to display the specific declined address or all of the declined addresses on the DHCP server.

**show ip dhcp declined** Field Descriptions

**Syntax**

`show ip dhcp declined [ip-address]`

**Parameters**

- `ip-address`—Specifies the IP address.

**Command Mode**

EXEC mode

**Example**

```
Router> show ip dhcp declined
DHCP server enabled
The number of declined entries is 2
IP address    Hardware address
172.16.1.11    00a0.9802.32de
172.16.3.254   02c7.f800.0422
```
Router> **show ip dhcp declined** 172.16.1.11

DHCP server enabled

The number of declined entries is 2

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.11</td>
<td>00a0.9802.32de</td>
</tr>
</tbody>
</table>

### 53.28 show ip dhcp expired

Use the `show ip dhcp expired` EXEC command to display the specific expired address or all of the expired addresses on the DHCP server.

**Syntax**

```
show ip dhcp expired [ip-address]
```

**Parameters**

- `ip-address`—Specifies the IP.

**Command Mode**

EXEC mode

**Example**

```
Router> **show ip dhcp expired**

DHCP server enabled

The number of expired entries is 1

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.11</td>
<td>00a0.9802.32de</td>
</tr>
<tr>
<td>172.16.3.254</td>
<td>02c7.f800.0422</td>
</tr>
</tbody>
</table>

Router> **show ip dhcp expired** 172.16.1.11

DHCP server enabled

The number of expired entries is 1

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.13</td>
<td>00a0.9802.32de</td>
</tr>
</tbody>
</table>
```
53.29  show ip dhcp pre-allocated

Use the show ip dhcp pre-allocated EXEC command to display the specific pre-allocated address or all the pre-allocated addresses on the DHCP server.

Syntax
show ip dhcp pre-allocated [ip-address]

Parameters
ip-address—Specifies the IP.

Command Mode
EXEC mode

Examples

Router> show ip dhcp pre-allocated
DHCP server enabled
The number of pre-allocated entries is 1
IP address   Hardware address
172.16.1.11   00a0.9802.32de
172.16.3.254  02c7.f800.0422
Router> show ip dhcp pre-allocated 172.16.1.11
DHCP server enabled
The number of pre-allocated entries is 1
IP address   Hardware address
172.16.1.15   00a0.9802.32de