Dell™ PowerConnect™ M6220 Systems

CLI Reference Guide

Notes, Notices, and Cautions

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

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

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

September 2007 Rev. 02

Contents

1 Command Groups

Introduction 1

Command Groups 1

Mode Types 4

Layer 2 Commands 5

Management ACL Commands 5

User Interface Commands 5

AAA Commands 5

Address Table Commands 6

Clock Commands 7

Denial of Service Commands 8

DHCP Filtering Commands 8

Ethernet Configuration Commands 9

GVRP Commands 10

IGMP Snooping Commands 10

IGMP Snooping Querier Commands 11

LACP Commands 11

Link Dependency Commands 12

LLDP Commands 12

Password Management 13

Port Monitor Commands 14

PHY Diagnostics Commands 14

System Management Commands 14

ACL Commands 16

Line Commands 16

IP Addressing Commands 17
802.1x Commands 17
Configuration and Image Files Commands 19
QoS Commands 19
Radius Commands 22
RMON Commands 23
SNMP Commands 24
Port Channel Commands 25
Spanning Tree Commands 25
SSH Commands 26
Syslog Commands 27
TACACS+ Commands 28
Telnet Server Commands 28
VLAN Commands 28
Web Server Commands 30
Layer 3 Commands 32
ARP Commands 32
DHCP and BOOTP Relay Commands 32
DHCPv6 Commands 33
DVMRP Commands 34
IGMP Commands 34
IGMP Proxy Commands 35
IP Routing Commands 36
IPv6 Routing Commands 36
Loopback Interface Commands 38
Multicast Commands 38
OSPF Commands 39
OSPFv3 Commands 42

PIM-DM Commands 44
PIM-SM Commands 45
Router Discovery Protocol Commands 46
Routing Information Protocol (RIP) Commands 46
Tunnel Interface Commands 47
Virtual LAN Routing Commands 48
Virtual Router Redundancy Commands 48

2 Using the CLI

Entering and Editing CLI Commands 50
CLI Command Modes 54
Starting the CLI 64
Using CLI Functions and Tools 71

3 Layer 2 Commands

4 Management ACL Commands

deny (management) 86
management access-class 87
management access-list 87
permit (management) 88
show management access-class 90
show management access-list 90

5 User Interface Commands

enable 94
end 95

exit (configuration) 95
exit (EXEC) 96

6 AAA Commands

aaa authentication enable 98
aaa authentication login 99
enable authentication 100
enable password 101
ip http authentication 101
ip https authentication 102
login authentication 103
password (Line Configuration) 104
password (User EXEC) 105
show authentication methods 105
show users accounts 106
show users login history 107
username 108

7 Address Table Commands

bridge address 110
bridge aging-time 111
bridge multicast address 111
bridge multicast filtering 112
bridge multicast forbidden address 113
bridge multicast forbidden forward-unregistered 114
bridge multicast forward-all 114
bridge multicast forward-unregistered 115

clear bridge 116
port security 116
port security max 117
show bridge address-table 118
show bridge address-table count 119
show bridge address-table static 120
show bridge multicast address-table 120
show bridge multicast filtering 121
show ports security 122
show ports security addresses 123

8 Clock Commands

show clock 126
show sntp configuration 126
show sntp status 127
sntp authenticate 128
sntp authentication-key 128
sntp broadcast client enable 129
sntp client poll timer 130
sntp server 130
sntp trusted-key 131
sntp unicast client enable 132
clock timezone hours-offset 132
no clock timezone 133
clock summer-time recurring 134
clock summer-time date 134
no clock summer-time recurring 135

show clock 136

9 Denial of Service Commands

dos-control firstfrag 140
dos-control icmp 140
dos-control l4port 141
dos-control sipdip 142
dos-control tcpflag 142
dos-control tcpfrag 143
show dos-control 143

10 DHCP Filtering Commands

ip dhcp filtering 146
ip dhcp filtering trust 146
show ip dhcp filtering 147

11 Ethernet Configuration Commands

clear counters. 150
description 150
duplex. 151
flowcontrol 151
interface ethernet 152
interface range ethernet 153
mdix. 153
mtu 154
negotiation 155
show interfaces advertise 155

show interfaces configuration 156
show interfaces counters 157
show interfaces description 160
show interfaces status 161
show statistics ethernet 163
show storm-control 167
shutdown 167
speed 168
storm-control broadcast 169
storm-control multicast 170
storm-control unicast 170

12 GVRP Commands

clear gvrp statistics 174
garp timer 174
gvrp enable (global) 175
gvrp enable (interface) 176
gvrp registration-forbid 176
gvrp vlan-creation-forbid 177
show gvrp configuration 178
show gvrp error-statistics 179
show gvrp statistics 180

13 IGMP Snooping Commands

ip igmp snooping (global) 184
ip igmp snooping (interface) 184
ip igmp snooping host-time-out 185

ip igmp snooping leave-time-out 185
ip igmp snooping mrouter-time-out 186
show ip igmp snooping groups 187
show ip igmp snooping interface 188
show ip igmp snooping mrouter 188
ip igmp snooping (VLAN) 190
ip igmp snooping fast-leave 190
ip igmp snooping groupmembership-interval 191
ip igmp snooping maxresponse 192
ip igmp snooping mcrtrexpiretime 192

14 IGMP Snooping Querier Commands

ip igmp snooping querier 196
ip igmp snooping querier query-interval 197
ip igmp snooping querier timer expiry 197
ip igmp snooping querier version 198
ip igmp snooping querier election participate 198
show igmpsnooping querier 199

15 LACP Commands

lacp port-priority 202
lacp system-priority 202
lacp timeout 203
show lacp ethernet 203
show lacp port-channel 205

16 Link Dependency Commands

link-dependency group 208

no link-dependency group 208

add ethernet 209

no add ethernet 209

add port-channel 210

no add port-channel 211

depends-on ethernet 211

no depends-on ethernet 212

depends-on port-channel 212

no depends-on port-channel 213

show link-dependency 213

17 LLDP Commands

clear lldp remote-data 216

clear lldp statistics 216

lldp notification 217

lldp notification-interval 217

lldp receive 218

lldp timers 218

lldp transmit 219

lldp transmit-mgmt 220

lldp transmit-tlv 220

show lldp 221

show lldp connections 222

show lldp interface 223

show lldp local-device 224

show lldp remote-device 226
show lldp statistics 227

18 Password Management Commands

passwords aging 232
passwords history 232
passwords lock-out 233
passwords min-length 234
show passwords configuration 234

19 Port Monitor Commands

monitor session 238
show monitor session 239

20 PHY Diagnostics Commands

show copper-ports cable-length 242
show copper-ports tdr 242
show fiber-ports optical-transceiver 243
test copper-port tdr 244

21 System Management Commands

asset-tag 249
cut-through mode 249
hostname 250
ip address 250
ip address none 251
ip address 251

member 252
movemanagement 253
no cut-through mode 253
no standby 254
ping 255
reload 256
set description 257
show boot-version 258
show cut-through mode 258
show ip interface out-of-band 259
show memory cpu 259
show process cpu 260
show sessions 262
show stack-port 263
show stack-port counters 264
show stack-port diag 266
show stack standby 267
show supported switchtype 268
show switch 271
show system 273
show system id 275
show users 275
show version 276
stack 277
standby 278
switch priority 278
switch renumber 279
telnet 279

traceroute 282

22 ACL Commands

access-list 286
deny | permit 287
ip access-group 288
no ip access-group 288
mac access-group 289
mac access-list extended 290
mac access-list extended rename 291
show ip access-lists 291
show mac access-list 292

23 Line Commands

exec-timeout 296
history 296
history size 297
line 297
show line 298
speed 299

24 IP Addressing Commands

clear host 302
helper-address 302
interface out-of-band 303
ip address 304
ip address dhcp 305

ip address vlan 305
ip default-gateway 306
ip domain-lookup 306
ip domain-name 307
ip helper-address 308
ip host 309
ip name-server 310
show arp switch 310
show hosts 311
show ip helper-address 312
show ip interface management 313

25 802.1x Commands

aaa authentication dot1x 316
dot1x max-req 316
dot1x port-control 317
dot1x re-authenticate 318
dot1x re-authentication 318
dot1x system-auth-control 319
dot1x timeout quiet-period 320
dot1x timeout re-authperiod 320
dot1x timeout server-timeout 321
dot1x timeout supp-timeout 322
dot1x timeout tx-period 323
show dot1x 323
show dot1x statistics 325
show dot1x users 327

dot1x auth-not-req 329
dot1x guest-vlan 329
dot1x guest-vlan enable 330
dot1x multiple-hosts 331
dot1x single-host-violation 331
show dot1x advanced 332

26 Configuration and Image File Commands

boot system 336
clear config 336
copy 337
delete backup-config 340
delete backup-image 340
delete startup-config 341
filedescr 341
ftpdownload 342
script apply 343
script delete 344
script list 344
script validate 346
show backup-config 346
show bootvar 347
show dir 348
show running-config 349
show startup-config 350
update bootcode 351

27 QoS Commands

assign-queue 355

class 355

class-map 356

class-map rename 357

classofservice dot1p-mapping 357

classofservice ip-dscp-mapping 358

classofservice trust 359

conform-color 359

cos-queue min-bandwidth 360

cos-queue strict 361

diffserv 361

drop 362

mark cos 363

mark ip-dscp 363

mark ip-precedence 364

match class-map 365

match cos 366

match destination-address mac 366

match dstip 367

match dstl4port 368

match ethertype 368

match ip dscp 369

match ip precedence 370

match ip tos 370

match protocol 371

match source-address mac 372

match srcip 372
match srcl4port 373
match vlan 374
mirror 374
police-simple 375
policy-map 376
redirect 377
service-policy 377
show class-map 378
show classofservice dot1p-mapping 379
show classofservice ip-dscp-mapping 380
show classofservice trust 383
show diffserv 383
show diffserv service interface ethernet in 384
show diffserv service interface port-channel in 385
show diffserv service brief 385
show interfaces cos-queue 386
show policy-map 388
show policy-map interface 389
show service-policy 390
traffic-shape 391

28 Radius Commands

auth-port 394
deadtime 394
key 395
priority 395

radius-server deadtime 396
radius-server host 397
radius-server key 397
radius-server retransmit 398
radius-server source-ip 399
radius-server timeout 399
retransmit 400
show radius-servers 401
source-ip 401
timeout 402
usage 403

29 RMON Commands

rmon alarm 406
rmon collection history 407
rmon event 408
rmon table-size 409
show rmon alarm 409
show rmon alarm-table 411
show rmon collection history 412
show rmon events 413
show rmon history 414
show rmon log 417
show rmon statistics 418

30 SNMP Commands

show snmp 422

show snmp engineID 423
show snmp filters 424
show snmp groups 425
show snmp users 426
show snmp views 427
snmp-server community 428
snmp-server community-group 429
snmp-server contact 430
snmp-server enable traps 431
snmp-server engineID local 431
snmp-server filter 432
snmp-server group 434
snmp-server host 435
snmp-server location 436
snmp-server trap authentication 437
snmp-server user 437
snmp-server view 439
snmp-server v3-host 439

31 Port Channel Commands

channel-group 442
interface port-channel 442
interface range port-channel 443
hashing-mode 444
no hashing-mode 444
show interfaces port-channel 445
show statistics port-channel 446

32 Spanning Tree Commands

abort (mst) 451

clear spanning-tree detected-protocols 451

exit (mst) 452

instance (mst) 452

name (mst) 453

revision (mst) 454

show (mst) 454

show spanning-tree 455

spanning-tree 465

spanning-tree bpdu 465

spanning-tree bpdu-protection 466

spanning-tree cost 467

spanning-tree disable 467

spanning-tree forward-time 468

spanning-tree hello-time 469

spanning-tree max-age 469

spanning-tree mode 470

spanning-tree mst configuration 471

spanning-tree mst cost 471

spanning-tree mst max-hops 472

spanning-tree mst port-priority 473

spanning-tree mst priority 473

spanning-tree portfast 474

spanning-tree port-priority 475

spanning-tree priority 476

spanning-tree root-protection 476

33 SSH Commands

crypto key generate dsa 480

crypto key generate rsa 480

crypto key pubkey-chain ssh 481

ip ssh port 482

ip ssh pubkey-auth 482

ip ssh server 483

key-string 483

show crypto key mypubkey 485

show crypto key pubkey-chain ssh 486

show ip ssh 487

user-key 487

34 Syslog Commands

clear logging 490

clear logging file 490

description 491

level 491

logging cli-command 492

logging 493

logging buffered 493

logging buffered size 494

logging console 495

logging facility 495

logging file 496

logging on 497

port 497

show logging 498
show logging file 500
show syslog-servers 500

35 TACACS+ Commands

key 504
port 504
priority 505
show tacacs 505
tacacs-server host 506
tacacs-server key 507
tacacs-server timeout 507
timeout 508

36 Telnet Server Commands

ip telnet server disable 509
ip telnet port 510
show ip telnet 510

37 VLAN Commands

dvlan-tunnel ethertype 513
interface vlan 513
interface range vlan 514
mode dvlan-tunnel 515
name 515
protocol group 516
protocol vlan group 517

protocol vlan group all . . . 517
show dvlan-tunnel . . . 518
show dvlan-tunnel interface . . . 519
show interfaces switchport . . . 520
show port protocol . . . 523
show switchport protected . . . 524
show vlan . . . 524
show vlan association mac . . . 525
show vlan association subnet . . . 526
switchport access vlan . . . 527
switchport forbidden vlan . . . 527
switchport general acceptable-frame-type tagged-only . . . 528
switchport general allowed vlan . . . 529
switchport general ingress-filtering disable . . . 529
switchport general pvid . . . 530
switchport mode . . . 531
switchport protected . . . 532
switchport protected name . . . 532
switchport trunk allowed vlan . . . 533
vlan . . . 534
vlan association mac . . . 534
vlan association subnet . . . 535
vlan database . . . 536
vlan makestatic . . . 536
vlan protocol group . . . 537
vlan protocol group add protocol . . . 538
vlan protocol group remove . . . 538

38 Web Server Commands

common-name 542

country 542

crypto certificate generate 543

crypto certificate import 544

crypto certificate request 545

duration 546

ip http port 547

ip http server 547

ip https certificate 548

ip https port 549

ip https server 549

key-generate 550

location 550

organization-unit 551

show crypto certificate mycertificate 552

show ip http 553

show ip https 553

state 554

39 Layer 3 Commands

40 ARP Commands

arp 560

arp cachesize 560

arp dynamicrenew 561

arp purge 561

arp resptime 562
arp retries 562
arp timeout 563
clear arp-cache 564
ip proxy-arp 564
show arp 565

41 DHCP and BOOTP Relay Commands

bootpdhcprelay cidridoptmode 568
bootpdhcprelay enable 568
bootpdhcprelay maxhopcount 569
bootpdhcprelay minwaittime 569
bootpdhcprelay serverip 570
show bootpdhcprelay 571

42 DHCPv6 Commands

clear ipv6 dhcp 574
dns-server 574
domain-name 575
ipv6 dhcp pool 576
ipv6 dhcp relay 576
ipv6 dhcp relay-agent-info-opt 577
ipv6 dhcp relay-agent-info-remote-id-subopt 578
ipv6 dhcp server 578
prefix-delegation 579
service dhcpv6 580
show ipv6 dhcp 581

show ipv6 dhcp binding 581
show ipv6 dhcp interface 582
show ipv6 dhcp pool 583
show ipv6 dhcp statistics 584

43 DVMRP Commands

ip dvmrp 588
ip dvmrp metric 588
ip dvmrp trapflags 589
show ip dvmrp 589
show ip dvmrp interface 590
show ip dvmrp neighbor 591
show ip dvmrp nexthop 591
show ip dvmrp prune 592
show ip dvmrp route 592

44 IGMP Commands

ip igmp 596
ip igmp last-member-query-count 596
ip igmp last-member-query-interval 597
ip igmp query-interval 597
ip igmp query-max-response-time 598
ip igmp robustness 599
ip igmp startup-query-count 599
ip igmp startup-query-interval 600
ip igmp version 601
show ip igmp 601

show ip igmp groups 602
show ip igmp interface 603
show ip igmp interface membership 604
show ip igmp interface stats 604
ip igmp router-alert-optional 605

45 IGMP Proxy Commands

ip igmp-proxy 608
ip igmp-proxy reset-status 608
ip igmp-proxy unsolicited-report-interval 609
show ip igmp-proxy 609
show ip igmp-proxy interface 610
show ip igmp-proxy groups 611
show ip igmp-proxy groups detail 612

46 IP Routing Commands

encapsulation 614
ip address 614
ip mtu 615
ip netdirbcast 616
ip route 616
ip route default 617
ip route distance 618
ip routing 619
routing 619
show ip brief 620
show ip interface 621

show ip protocols 622
show ip route 624
show ip route preferences 624
show ip route summary 625
show ip stats 626

47 IPv6 Routing Commands

clear ipv6 neighbors 631
clear ipv6 statistics 631
ipv6 address 632
ipv6 enable 633
ipv6 forwarding 633
ipv6 mtu 634
ipv6 nd dad attempts 635
ipv6 nd managed-config-flag 635
ipv6 nd ns-interval 636
ipv6 nd other-config-flag 637
ipv6 nd prefix 637
ipv6 nd ra-interval 639
ipv6 nd ra-lifetime 639
ipv6 nd reachable-time 640
ipv6 nd suppress-ra 641
ipv6 route 641
ipv6 route distance 642
ipv6 unicast-routing 643
ping ipv6 643
ping ipv6 interface 644

show ipv6 brief 645
show ipv6 interface 646
show ipv6 neighbors 647
show ipv6 route 648
show ipv6 route preferences 649
show ipv6 route summary 650
show ipv6 traffic 651
show ipv6 vlan 653
traceroute ipv6 654

48 Loopback Interface Commands

interface loopback 656
show interfaces loopback 656

49 Multicast Commands

ip mcast boundary 660
ip multicast 660
ip multicast staticroute 661
ip multicast ttl-threshold 662
mrinfo 663
mstat 663
mtrace 664
no ip mcast mroute 665
show ip mcast 665
show ip mcast boundary 666
show ip mcast interface 667
show ip mcast mroute 668

show ip mcast mroute group 669
show ip mcast mroute source 670
show ip mcast mroute static 671
show mrinfo 671
show mstat 672
show mtrace 673

50 OSPF Commands

area default-cost 677
area nssa 677
area nssa default-info-originate 678
area nssa no-redistribute 679
area nssa no-summary 679
area nssa translator-role 680
area nssa translator-stab-intv 681
area range 681
area stub 682
area stub no-summary 683
area virtual-link 684
area virtual-link authentication 684
area virtual-link dead-interval 685
area virtual-link hello-interval 686
area virtual-link retransmit-interval 687
area virtual-link transmit-delay 687
default-information originate 688
default-metric 689
distance ospf 689

distribute-list out 690
enable 691
exit-overflow-interval 691
external-lsdb-limit 692
ip ospf 693
ip ospf areaid 693
ip ospf authentication 694
ip ospf cost 695
ip ospf dead-interval 695
ip ospf hello-interval 696
ip ospf mtu-ignore 696
ip ospf priority 697
ip ospf retransmit-interval 698
ip ospf transmit-delay 699
maximum-paths 699
redistribute 700
router-id 701
router ospf 701
show ip ospf 702
show ip ospf abr 703
show ip ospf area 704
show ip ospf asbr 705
show ip ospf database 706
show ip ospf database database-summary 707
show ip ospf interface 709
show ip ospf interface brief 710
show ip ospf interface stats 711
show ip ospf neighbor 711

show ip ospf range 712
show ip ospf statistics 713
show ip ospf stub table 714
show ip ospf virtual-link 715
show ip ospf virtual-link brief 716
timers spf 716
trapflags 717
1583compatibility 717

51 OSPFv3 Commands

area default-cost 721
area nssa 721
area nssa default-info-originate 722
area nssa no-redistribute 723
area nssa no-summary 723
area nssa translator-role 724
area nssa translator-stab-intv 725
area range 725
area stub 726
area stub no-summary 727
area virtual-link 728
area virtual-link dead-interval 728
area virtual-link hello-interval 729
area virtual-link retransmit-interval 730
area virtual-link transmit-delay 730
default-information originate 731
default-metric 732

distance ospf 733
enable 733
exit-overflow-interval 734
external-lsdb-limit 735
ipv6 ospf 735
ipv6 ospf areaid 736
ipv6 ospf cost 737
ipv6 ospf dead-interval 737
ipv6 ospf hello-interval 738
ipv6 ospf mtu-ignore 739
ipv6 ospf network 739
ipv6 ospf priority 740
ipv6 ospf retransmit-interval 741
ipv6 ospf transmit-delay 741
ipv6 router ospf 742
maximum-paths 743
redistribute 743
router-id 744
show ipv6 ospf 745
show ipv6 ospf abr 746
show ipv6 ospf area 746
show ipv6 ospf asbr 747
show ipv6 ospf database 748
show ipv6 ospf database database-summary 751
show ipv6 ospf interface 752
show ipv6 ospf interface brief 753
show ipv6 ospf interface stats 754
show ipv6 ospf interface vlan 755

show ipv6 ospf neighbor 757
show ipv6 ospf range 758
show ipv6 ospf stub table 758
show ipv6 ospf virtual-link 759
show ipv6 ospf virtual-link brief 760
trapflags 761

52 PIM-DM Commands

ip pimdm 764
ip pimdm mode 764
ip pimdm query-interval 765
show ip pimdm 765
show ip pimdm interface 766
show ip pimdm interface stats 767
show ip pimdm neighbor 767

53 PIM-SM Commands

ip pimsm 770
ip pimsm cbsrhashmasklength 770
ip pimsm cbsrpreference 771
ip pimsm crppreference 771
ip pimsm message-interval 772
ip pimsm mode 773
ip pimsm query-interval 773
ip pimsm register-rate-limit 774
ip pimsm spt-threshold 775
ip pimsm staticrp 775

ip pim-trapflags 776
show ip pimsm 776
show ip pimsm componenttable 777
show ip pimsm interface 778
show ip pimsm interface stats 779
show ip pimsm neighbor 779
show ip pimsm rp 780
show ip pimsm rphash 781
show ip pimsm staticrp 781

54 Router Discovery Protocol Commands

ip irdp 784
ip irdp address 784
ip irdp holdtime 785
ip irdp maxadvertinterval 785
ip irdp minadvertinterval 786
ip irdp preference 787
show ip irdp 787

55 Routing Information Protocol (RIP) Commands

auto-summary 790
default-information originate 790
default-metric 791
distance rip 791
distribute-list out 792
enable 793
hostroutesaccept 793

ip rip 794
ip rip authentication 794
ip rip receive version 795
ip rip send version 796
redistribute 796
router rip 797
show ip rip 798
show ip rip interface 799
show ip rip interface brief 800
split-horizon 801

56 Tunnel Interface Commands

interface tunnel 804
show interfaces tunnel 804
tunnel destination 805
tunnel mode ipv6ip 806
tunnel source 806

57 Virtual LAN Routing Commands

show ip vlan 810
vlan routing 810

58 Virtual Router Redundancy Protocol Commands

ip vrrp 814
ip vrrp authentication 814
ip vrrp ip 815
ip vrrp mode 816

ip vrrp preempt 817
ip vrrp priority 817
ip vrrp timers advertise 818
show ip vrrp 819
show ip vrrp interface 819
show ip vrrp interface brief 820
show ip vrrp interface stats 821

1

Command Groups

Introduction

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

A switch can be configured and maintained by entering commands from the CLI, which is based solely on textual input and output with commands being entered by a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a console terminal connected to an EIA/TIA-232 port or through a Telnet session.

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

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

Command Groups

The system commands can be broken down into two sets of functional groups, Layers 2 and 3.

Command Group	Description
Layer 2 Groups	
AAA	Configures connection security including authorization and passwords.
ACL	Configures and displays ACL information.
Address Table	Configures bridging address tables.
Clock	Configures the system clock.
Configuration and Image Files	Manages the switch configuration files.
Denial of Service	Provides several Denial of Service options.

Command Group	Description
DHCP Filtering	Configures DHCP filtering and whether an interface is trusted for filtering.
Ethernet Configuration	Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.
GVRP	Configures and displays GVRP configuration and information.
IGMP Snooping	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IGMP Snooping Querier	Configures IGMP Snooping Querier and displays IGMP Snooping Querier information.
IP Addressing	Configures and manages IP addresses on the switch.
LACP	Configures and displays LACP information.
Link Dependency	Configures and displays link dependency information.
Line	Configures the console, SSH, and remote Telnet connection.
LLDP	Configures and displays LLDP information.
Management ACL	Configures and displays management access-list information.
Password Management	Provides password management.
PHY Diagnostics	Diagnoses and displays the interface status.
Port Channel	Configures and displays Port channel information.
Port Monitor	Monitors activity on specific target ports.
QoS	Configures and displays QoS information.
RADIUS	Configures and displays RADIUS information.
RMON	Can be configured through the CLI and displays RMON information.
SNMP	Configures SNMP communities, traps and displays SNMP information.
Spanning Tree	Configures and reports on Spanning Tree protocol.
SSH	Configures SSH authentication.
Syslog Commands	Manages and displays syslog messages.
System Management	Configures the switch clock, name and authorized users.
TACACS+	Configures and displays TACACS+ information.
User Interface	Describes user commands used for entering CLI commands.
VLAN	Configures VLANs and displays VLAN information.
Web Server	Configures Web based access to the switch.

Command Group	Description
Telnet Server	Configures Telnet service on the switch and displays Telnet information.
802.1x	Configures and displays commands related to 802.1x security protocol.
Layer 3 Groups	
ARP (IPv4)	Manages Address Resolution Protocol functions.
DHCP and BOOTP Relay (IPv4)	Manages DHCP/BOOTP operations on the system.
DHCPv6 (IPv6)	Configures IPv6 DHCP functions.
DVMRP (Mcast)	Configures DVMRP operations.
IGMP (Mcast)	Configures IGMP operations.
IGMP Proxy (Mcast)	Manages IGMP Proxy on the system.
IP Routing (IPv4)	Configures IP routing and addressing.
IPv6 Routing (IPv6)	Configures IPv6 routing and addressing.
Loopback Interface (IPv6)	Manages Loopback configurations.
Multicast (Mcast)	Manages Multicasting on the system.
OSPF (IPv4)_	Manages shortest path operations.
OSPFv3 (IPv6)	Manages IPv6 shortest path operations.
PIM-DM (Mcast)	Configures PIM-DM operations.
PIM-SM (Mcast)	Configures PIM-SM operations.
Router Discovery Protocol (IPv4)	Manages router discovery operations.
Routing Information Protocol (IPv4)	Configures RIP activities.
Tunnel Interface (IPv6)	Managing tunneling operations.
Virtual LAN Routing (IPv4)	Controls virtual LAN routing.
Virtual Router Redundancy (IPv4)	Manages router redundancy on the system.

Mode Types

The tables on the following pages use these abbreviations for Command Mode names.

- CC — Crypto Configuration
- CMC — Class-Map Configuration
- GC — Global Configuration
- IC — Interface Configuration
- IP — IP Access List Configuration
- KC - Key Chain
- KE — Key
- L — Logging
- LC — Line Configuration
- MA — Management Access-level
- MC — MST Configuration
- ML — MAC-List Configuration
- MT — MAC-acl
- PE — Privileged EXEC
- PM — Policy Map Configuration
- PCGC — Policy Map Global Configuration
- PCMC — Policy Class Map Configuration
- R — Radius
- RIP— Router RIP Configuration
- ROSPF—Router Open Shortest Path First
- ROSV3—Router Open Shortest Path First Version 3
- SG — Stack Global Configuration
- SP — SSH Public Key
- SK — SSH Public Key-chain
- TC — TACACS Configuration
- UE — User EXEC
- VLAN—VLAN Configuration
- v6DP—IPv6 DHCP Pool Configuration

Layer 2 Commands

Management ACL Commands

Command	Description	Mode*
deny (management)	Defines a deny rule.	MA
management access-class	Defines which management access-list is used.	GC
management access-list	Defines a management access-list, and enters the access-list for configuration.	GC
permit (management)	Defines a permit rule.	MA
show management access-class	Displays the active management access-list.	PE
show management access-list	Displays management access-lists.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

User Interface Commands

Command	Description	Mode*
enable	Enters the privileged EXEC mode.	UE
end	Gets the CLI user control back to the privileged execution mode or user execution mode.	Any
exit(configuration)	Exits any configuration mode to the previously highest mode in the CLI mode hierarchy.	(All)
exit(EXEC)	Closes an active terminal session by logging off the switch.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

AAA Commands

Command	Description	Mode*
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.	GC
aaa authentication login	Defines login authentication.	GC
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.	LC
enable password	Sets a local password to control access to the normal level.	GC
ip http authentication	Specifies authentication methods for http.	GC

Command	Description	Mode*
ip https authentication	Specifies authentication methods for https.	GC
login authentication	Specifies the login authentication method list for a remote telnet or console.	LC
password	Specifies a password on a line.	LC
password	Specifies a user password	UE
show authentication methods	Shows information about authentication methods	PE
show user accounts	Displays information about the local user database	PE
show users login-history	Displays information about login histories of users	PE
username	Establishes a username-based authentication system.	GC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Address Table Commands

Command	Description	Mode*
bridge address	Adds a static MAC-layer station source address to the bridge table.	IC
bridge aging-time	Sets the address table aging time.	GC
bridge multicast address	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.	IC
bridge multicast filtering	Enables filtering of Multicast addresses.	GC
bridge multicast forbidden address	Forbids adding a specific Multicast address to specific ports.	IC
bridge multicast forbidden forward-unregistered	Forbids a port to be a forwarding-unregistered-multicast-addresses port.	IC
bridge multicast forward-all	Enables forwarding of all Multicast packets on a port.	IC
bridge multicast forward-unregistered	Enables the forwarding of unregistered multicast addresses	IC
clear bridge	Removes any learned entries from the forwarding database.	PE
port security	Disables new address learning on an interface.	IC
port security max	Configures the maximum addresses that can be learned on the port while the port is in port security mode.	IC
show bridge address-table	Displays dynamically created entries in the bridge-forwarding database.	PE

Command	Description	Mode*
show bridge address-table count	Displays the number of addresses present in the Forwarding Database.	PE
show bridge address-table static	Displays statically created entries in the bridge-forwarding database.	PE
show bridge multicast address-table	Displays Multicast MAC address table information.	PE
show bridge multicast filtering	Displays the Multicast filtering configuration.	PE
show ports security	Displays the port-lock status.	PE
show ports security addresses	Displays current dynamic addresses in locked ports.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Clock Commands

Command	Description	Mode*
show clock	Displays the time and date of the system clock.	UE
show sntp configuration	Displays the SNTP configuration.	PE
show sntp status	Displays the SNTP status.	PE
sntp authenticate	Set to require authentication for received NTP traffic from servers.	GC
sntp authentication-key	Defines an authentication key for SNTP.	GC
sntp broadcast client enable	Enables SNTP Broadcast clients.	GC
sntp client enable	Enables SNTP Broadcast and Anycast clients on an interface.	IC
sntp client poll timer	Defines polling time for the SNTP client.	GC
sntp server	Configures the SNTP server to use SNTP to request and accept NTP traffic from it.	
sntp trusted-key	Authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize.	GC
sntp unicast client enable	Enables clients to use Simple Network Time Protocol (SNTP) predefined Unicast clients.	GC
clock timezone hours-offset	Sets the offset to Coordinated Universal Time.	GC
no clock timezone	Resets the time zone settings.	GC
clock summer-time recurring	Sets the summertime offset to UTC recursively every year.	GC
clock summer-time date	Sets the summertime offset to UTC.	GC

Command	Description	Mode*
no clock summer-time recurring	Resets the recurring summertime configuration.	GC
show **clock**	Displays the time and date from the system clock.	EXEC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Denial of Service Commands

Command	Description	Mode*
dos-control firstfrag	Enables Minimum TCP Header Size Denial of Service protection.	GC
dos-control icmp	Enables Maximum ICMP Packet Size Denial of Service protections.	GC
dos-control l4port	Enables L4 Port Denial of Service protection.	GC
dos-control sipdip	Enables Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection.	GC
dos-control tcpflag	Enables TCP Flag Denial of Service protections.	GC
dos-control tcpfrag	Enables TCP Fragment Denial of Service protection.	GC
show dos-control	Displays Denial of Service configuration information.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

DHCP Filtering Commands

Command	Description	Mode*
ip dhcp filtering	Enables DHCP filtering globally.	GC
ip dhcp filtering trust	Configures an interface as trusted for DHCP filtering purposes	IC
show ip dhcp filtering	Displays the DHCP filtering configuration.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Ethernet Configuration Commands

Command	Description	Mode*
clear counters	Clears statistics on an interface.	PE
description	Adds a description to an interface.	IC
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	IC
flowcontrol	Configures the flow control on a given interface.	GC
interface ethernet	Enters the interface configuration mode to configure an Ethernet type interface.	GC
interface range ethernet	Enters the interface configuration mode to configure multiple Ethernet type interfaces.	GC
mdix	Enables automatic crossover on a given interface.	IC
mtu	Enables jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU).	IC
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.	IC
show interfaces advertise	Displays information about auto negotiation advertisement.	PE
show interfaces configuration	Displays the configuration for all configured interfaces.	UE
show interfaces counters	Displays traffic seen by the physical interface.	UE
show interfaces description	Displays the description for all configured interfaces.	UE
show interfaces status	Displays the status for all configured interfaces.	UE
show statistics ethernet	Displays statistics for one port or for the entire switch.	PE
show storm-control	Displays the storm control configuration.	PE
shutdown	Disables interfaces.	IC
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	IC
storm-control broadcast	Enables Broadcast storm control.	IC
storm-control multicast	Enables the switch to count Multicast packets together with Broadcast packets.	IC
storm-control unicast	Enables Unicast storm control.	IC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

GVRP Commands

Command	Description	Mode*
clear gvrp statistics	Clears all the GVRP statistics information.	PE
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.	IC
gvrp enable (global)	Enables GVRP globally.	GC
gvrp enable (interface)	Enables GVRP on an interface.	IC
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	IC
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.	IC
show gvrp configuration	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP	PE
show gvrp error-statistics	Displays GVRP error statistics.	UE
show gvrp statistics	Displays GVRP statistics.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IGMP Snooping Commands

Command	Description	Mode*
ip igmp snooping (Global)	In Global Config mode, Enables Internet Group Management Protocol (IGMP) snooping.	GC VLAN
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	IC
ip igmp snooping host-time-out	Configures the host-time-out.	IC
ip igmp snooping leave-time-out	Configures the leave-time-out.	IC
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.	IC
show ip igmp snooping groups	Displays Multicast groups learned by IGMP snooping.	UE
show ip igmp snooping interface	Displays IGMP snooping configuration.	PE
show ip igmp snooping mrouter	Displays information on dynamically learned Multicast router interfaces.	PE
ip igmp snooping (VLAN)	In VLAN Config mode, enables IGMP snooping on a particular VLAN or on all interfaces participating in a VLAN.	GC VLAN

Command	Description	Mode*
ip igmp snooping fast-leave	Enables or disables IGMP Snooping fast-leave mode on a selected VLAN.	VLAN
ip igmp snooping groupmembership-interval	Sets the IGMP Group Membership Interval time on a VLAN.	VLAN
ip igmp snooping maxresponse	Sets the IGMP Maximum Response time on a particular VLAN.	VLAN
ip igmp snooping mcrtrexpiretime	Sets the Multicast Router Present Expiration time.	VLAN
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IGMP Snooping Querier Commands

Command	Description	Mode*
ip igmp snooping querier	Enables/disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN.	GC, VLAN
ip igmp snooping querier query-interval	Sets the IGMP Querier Query Interval time.	GC
ip igmp snooping querier timer expiry	Sets the IGMP Querier timer expiration period.	GC
ip igmp snooping querier version	Sets the IGMP version of the query that the snooping switch is going to send periodically.	GC
ip igmp snooping querier election participate	Enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN.	VLAN
show igmpsnooping querier	Displays IGMP Snooping Querier information.	PE

LACP Commands

Command	Description	Mode*
lacp port-priority	Configures the priority value for physical ports.	IC
lacp system-priority	Configures the system LACP priority.	GC
lacp timeout	Assigns an administrative LACP timeout.	IC
show lacp ethernet	Displays LACP information for Ethernet ports.	PE
show lacp port-channel	Displays LACP information for a port-channel.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Link Dependency Commands

Command	Description	Mode*
link-dependency group	Enters the link-dependency mode to configure a link-dependency group.	Link Dependency
no link-dependency group	Removes the configuration for a link-dependency group.	Link Dependency
add ethernet	Adds member Ethernet port(s) to the dependency list.	Link Dependency
no add ethernet	Removes member Ethernet port(s) from the dependency list.	Link Dependency
add port-channel	Adds member port-channels to the dependency list.	Link Dependency
no add port-channel	Removes member port-channels from the dependency list.	Link Dependency
depends-on ethernet	Adds the dependent Ethernet ports list.	Link Dependency
no depends-on ethernet	Removes the dependent Ethernet ports list.	Link Dependency
depends-on port-channel	Adds the dependent port-channels list.	Link Dependency
no depends-on port-channel	Removes the dependent port-channels list.	Link Dependency
show link-dependency	Shows the link dependencies configured on a particular group.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

LLDP Commands

Command	Description	Mode*
clear lldp remote data	Deletes all data from the remote data table.	PE
clear lldp statistics	Resets all LLDP statistics.	PE
lldp notification	Enables remote data change notifications.	IC
lldp notification-interval	Limits how frequently remote data change notifications are sent.	GC
lldp receive	Enables the LLDP receive capability.	IC
lldp timers	Sets the timing parameters for local data transmission on ports enabled for LLDP.	GC

Command	Description	Mode*
lldp transmit	Enables the LLDP advertise capability.	IC
lldp transmit-mgmt	Specifies that transmission of the local system management address information in the LLDPDUs is included.	IC
lldp transmit-tlv	Specifies which optional TLVs in the 802.1AB basic management set will be transmitted in the LLDPDUs.	IC
show lldp	Displays the current LLDP configuration summary.	PE
show lldp connections	Displays the current LLDP remote data.	PE
show lldp interface	Displays the current LLDP interface state.	PE
show lldp local-device	Displays the LLDP local data	PE
show lldp remote-device	Displays the LLDP remote data	PE
show lldp statistics	Displays the current LLDP traffic statistics.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Password Management

Command	Description	Mode*
passwords aging	Implements aging on the passwords such that users are required to change passwords when they expire.	GC
passwords history	Enables the administrator to set the number of previous passwords that are stored to ensure that users do not reuse their passwords too frequently.	GC
passwords lock-out	Enables the administrator to strengthen the security of the switch by enabling the user lockout feature. When a lockout count is configured, a user who is logging in must enter the correct password within that count.	GC
passwords min-length	Enables the administrator to enforce a minimum length required for a password.	GC
show passwords configuration	Displays the configuration parameters for password configuration.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Port Monitor Commands

Command	Description	Mode*
monitor session	Configures a port monitoring session.	GC
show monitor session	Displays the port monitoring status.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.*		

PHY Diagnostics Commands

Command	Description	Mode*
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.	PE
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.	PE
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.	PE
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.*		

System Management Commands

Command	Description	Mode*
asset-tag	Specifies the switch asset-tag.	GC
cut-through mode	Enables the cut-through mode on the switch.	GC
hostname	Specifies or modifies the switch host name.	GC
ip address	Sets a static OOB port IP address.	IC (out-of-band)
ip address none	Disables DHCP/BOOTP on the OOB port.	IC (out-of-band)
ip address {dhcp/bootp}	Enables DHCP/BOOTP on the OOB port.	IC (out-of-band)
member	Configures the switch.	SG
movemanagement	Moves the Management Switch functionality from one switch to another.	GC

Command	Description	Mode*
no cut-through mode	Disables the cut-through mode on the switch.	GC
no standby	Unconfigures the standby in the stack.	Stack GC
ping	Sends ICMP echo request packets to another node on the network.	UE
reload	Reloads the operating system.	PE
set description	Associates a text description with a switch in the stack.	GC
show boot-version	Displays the boot image version details.	PE
show cut-through mode	Show the cut-through mode on the switch.	PE
show ip interface out-of-band	Disables DHCP/BOOTP on the OOB port.	PE
show memory cpu	Checks the total and available RAM space on the switch.	PE
show process cpu	Checks the CPU utilization for each process currently running on the switch.	PE
show sessions	Displays a list of the open telnet sessions to remote hosts.	PE
show stack-port	Displays summary stack-port information for all interfaces.	PE
show stack-port counters	Displays summary data counter information for all interfaces.	PE
show stack-port diag	Displays front panel stacking diagnostics for each port.	PE
show stack-standby	Shows the Standby configured in the stack.	PE
show supported switchtype	Displays information about all supported switch types.	UE
show switch	Displays information about the switch status.	UE
show system	Displays system information.	UE
show system id	Displays the service ID information.	UE
show users	Displays information about the active users.	PE
show version	Displays the system version information.	UE
stack	Sets the mode to Stack Global Config.	GC
standby	Configures the standby in the stack.	Stack GC
switch priority	Configures the ability of the switch to become the Management Switch.	GC
switch renumber	Changes the identifier for a switch in the stack.	GC
telnet	Logs into a host that supports Telnet.	PE
traceroute	Discovers the IP routes that packets actually take when travelling to their destinations.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

ACL Commands

Command	Description	Mode*
access-list	Creates an Access Control List (ACL) that is identified by the parameter *accesslistnumber*.	IC
deny|permit	The deny command denies traffic if the conditions defined in the deny statement are matched. The permit command allows traffic if the conditions defined in the permit statement are matched.	ML
ip access-group	Attaches a specified access-control list to an interface.	GC or IC
ip access-group <name> out	Applies an IP based egress ACL on an Ethernet interface or a group of interfaces.	IC
mac access-group	Attaches a specific MAC Access Control List (ACL) to an interface in a given direction.	GC or IC
mac access-list extended	Creates the MAC Access Control List (ACL) identified by the *name* parameter.	GC
mac access-list extended rename	Renames the existing MAC Access Control List (ACL) name.	GC
show ip access-lists	Displays an Access Control List (ACL) and all of the rules that are defined for the ACL.	PE
show mac access-list	Displays a MAC access list and all of the rules that are defined for the ACL.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Line Commands

Command	Description	Mode*
exec-timeout	Configures the interval that the system waits for user input.	LC
history	Enables the command history function.	UE
history size	Changes the command history buffer size for a particular line.	UE
line	Identifies a specific line for configuration and enters the line configuration command mode.	GC
show line	Displays line parameters.	UE
speed	Sets the line baud rate.	LC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IP Addressing Commands

Command	Description	Mode*
clear host	Deletes entries from the host name-to-address cache	PE
helper address	Enable forwarding User Datagram Protocol (UDP) Broadcast packets received on an interface.	IC
interface out-of-band	Brings up the OOB port configuration menu.	GC
ip address	Sets a management IP address on the switch.	GC
ip address dhcp	Acquires an IP address on an interface from the DHCP server.	GC
ip address vlan	Sets the management VLAN.	GC
ip default-gateway	Defines a default gateway (router).	GC
ip domain-lookup	Enables IP DNS-based host name-to-address translation.	GC
ip domain-name	Defines a default domain name to complete unqualified host names.	GC
ip helper address	Allows the device to forward User Datagram Protocol (UDP) broadcasts received on an interface.	GC
ip host	Configures static host name-to-address mapping in the host cache.	GC
ip name-server	Configures available name servers.	GC
show arp switch	Displays the entries in the ARP table.	PE
show hosts	Displays the default domain name, a list of name server hosts, static and cached list of host names and addresses.	PE
show ip helper address	Displays the ip helper addresses configuration.	PE
show ip interface management	Displays the management IP interface information.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

802.1x Commands

Command	Description	Mode*
aaa authentication dot1x	Specifies one or more authentication, authorization and accounting (AAA) methods for use on interfaces running IEEE 802.1X.	GC
dot1x max-req	Sets the maximum number of times the switch sends an EAP-request frame to the client before restarting the authentication process.	IC

Command	Description	Mode*
dot1x port-control	Enables manual control of the authorization state of the port.	IC
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1x-enabled ports or a specified 802.1X enabled port.	PE
dot1x re-authentication	Enables periodic re-authentication of the client.	IC
dot1x system-auth-control	Enables 802.1X globally.	GC
dot1x timeout quiet-period	Sets the number of seconds the switch remains in the quiet state following a failed authentication attempt	IC
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.	IC
dot1x timeout server-timeout	Sets the number of seconds the switch waits for a response from the authentication server before resending the request.	IC
dot1x timeout supp-timeout	Sets the number of seconds the switch waits for a response to an EAP-request frame from the client before retransmitting the request.	IC
dot1x timeout tx-period	Sets the number of seconds the switch waits for a response to an EAP-request/identify frame from the client before resending the request.	IC
show dot1x	Displays 802.1X status for the switch or the specified interface.	PE
show dot1x statistics	Displays 802.1X statistics for the specified interface.	PE
show dot1x users	Displays active 802.1X authenticated users for the switch.	PE
dot1x auth-not-req	Enables unauthorized users to access that VLAN.	IC
dot1x guest-vlan	Defines a guest VLAN.	IC
dot1x guest-vlan enable	Enables unauthorized users on an interface an access to the guest VLAN.	IC
dot1x multiple-hosts	Allows multiple hosts (clients) on an 802.1x-authorized port where the dot1x port-control interface configuration command is set to auto.	IC
dot1x single-host-violation	Configures the action to be taken when a station with a MAC address that is not the supplicant MAC address attempts to access the interface.	IC
show dot1x advanced	Displays 802.1X advanced features for the switch or specified interface.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Configuration and Image Files Commands

Command	Description	Mode*
boot system	Specifies the system image that the switch loads at startup.	PE
clear config	Restores switch to default configuration	PE
copy	Copies files from a source to a destination.	PE
delete backup-image	Deletes a file from a flash memory.	PE
delete backup-config	Deletes the backup configuration file	PE
delete startup-config	Deletes the startup configuration file.	PE
filedescr	Adds a description to a file.	PE
ftpdownload	Updates the backup image on the switch.	PE
script apply	Applies commands in the script to the switch.	PE
script delete	Deletes a specific script.	PE
script list	Lists all scripts present in the switch.	PE
script show	Displays the contents of a script file.	PE
script validate	Validates a script file.	PE
show backup-config	Displays contents of a backup configuration file	PE
show bootvar	Displays the active system image file that the switch loads at startup.	UE
show dir	Lists all the files available on the flash file system.	PE
show running-config	Displays the contents of the currently running configuration file.	PE
show startup-config	Displays the startup configuration file contents.	PE
update bootcode	Updates the bootcode on one or more switches.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

QoS Commands

Command	Description	Mode*
assign-queue	Modifies the queue ID to which the associated traffic stream is assigned.	PCMC
class	Creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.	PMC

Command	Description	Mode*
class-map	Defines a new DiffServ class of type *match-all*, *match-any*, or *match-access-group*. For now, only *match-all* is available in the CLI.	GC
class-map rename	Changes the name of a DiffServ class.	GC
classofservice dotlp-mapping	Maps an 802.1p priority to an internal traffic class for a switch.	GC and IC
classofservice ip-dscp-mapping	Maps an IP DSCP value to an internal traffic class.	GC
classofservice trust	Sets the class of service trust mode of an interface.	GC and IC
conform-color	Specifies for each outcome, the only possible actions are drop, set-cos-transmit, set-sec-cos-transmit, setdscp-transmit, set-prec-transmit, or transmit	PCMC
cos-queue min-bandwidth	Specifies the minimum transmission bandwidth for each interface queue.	GC and IC
cos-queue strict	Activates the strict priority scheduler mode for each specified queue.	GC and IC
diffserv	Sets the DiffServ operational mode to active.	GC
drop	Use the **drop** policy-class-map configuration command to specify that all packets for the associated traffic stream are to be dropped at ingress.	PCMC
mark cos	Marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header.	PCMC
mark ip-dscp	Marks all packets for the associated traffic stream with the specified IP DSCP value.	PCMC
mark ip-precedence	Marks all packets for the associated traffic stream with the specified IP precedence value.	PCMC
match class-map	Adds add to the specified class definition the set of match conditions defined for another class.	CMC
match cos	Adds to the specified class definition a match condition for the Class of Service value.	CMC
match destination-address mac	Adds to the specified class definition a match condition based on the destination MAC address of a packet.	CMC
match dstip	Adds to the specified class definition a match condition based on the destination IP address of a packet.	CMC

Command	Description	Mode*
match dstl4port	Adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword, or a numeric notation.	CMC
match ethertype	Adds to the specified class definition a match condition based on the value of the ethertype.	CMC
match ip dscp	Adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet.	CMC
match ip precedence	Adds to the specified class definition a match condition based on the value of the IP.	CMC
match ip tos	Adds to the specified class definition a match condition based on the value of the IP TOS field in a packet.	CMC
match protocol	Adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.	CMC
match source-address mac	Adds to the specified class definition a match condition based on the source MAC address of the packet.	CMC
match srcip	Adds to the specified class definition a match condition based on the source IP address of a packet.	CMC
match srcl4port	Adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword, a numeric notation, or a numeric range notation.	CMC
match vlan	Adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field.	CMC
mirror	Mirrors all the data that matches the class defined to the destination port specified	PCMC
police-simple	Establishes the traffic policing style for the specified class.	PCMC
policy-map	Establishes a new DiffServ policy	GC
redirect	Specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).	PCMC
service-policy	Attaches a policy to an interface in a particular direction.	GC and IC
show class-map	Displays all configuration information for the specified class.	PE
show classofservice dotlp-mapping	Displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.	PE

Command	Description	Mode*
show classofservice ip-dscp-mapping	Displays the current IP DSCP mapping to internal traffic classes for a specific interface.	PE
show classofservice trust	Displays the current trust mode setting for a specific interface.	PE
show diffserv	Displays the DiffServ General Status information.	PE
show diffserv service interface ethernet in	Displays policy service information for the specified interface and direction.	PE
show diffserv service interface port-channel in	Displays policy service information for the specified interface and direction.	PE
show diffserv service brief	Displays all interfaces in the system to which a DiffServ policy has been attached.	PE
show interfaces cos-queue	Displays the class-of-service queue configuration for the specified interface.	PE
show policy-map	Displays all configuration information for the specified policy.	PE
show policy-map interface	Displays policy-oriented statistics information for the specified interface and direction	PE
show service-policy	Displays a summary of policy-oriented statistics information for all interfaces in the specified direction.	PE
traffic-shape	Specifies the maximum transmission bandwidth limit for the interface as a whole.	GC and IC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Radius Commands

Command	Description	Mode*
auth-port	Sets the port number for authentication requests of the designated radius server.	R
deadtime	Improves Radius response times when a server is unavailable by causing the unavailable server to be skipped.	R
key	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.	R
priority	Specifies the order in which the servers are to be used, with 0 being the highest priority.	R
radius-server deadtime	Improves RADIUS response times when servers are unavailable. Causes the unavailable servers to be skipped.	GC

radius-server host	Specifies a RADIUS server host.	GC
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.	GC
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	GC
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	GC
radius-server timeout	Sets the interval for which a switch waits for a server host to reply	GC
retransmit	Specifies the number of times the software searches the list of RADIUS server hosts before stopping the search.	R
show radius-servers	Displays the RADIUS server settings.	PE
source-ip	Specifies the source IP address to be used for communication with RADIUS servers.	R
timeout	Sets the timeout value in seconds for the designated radius server.	R
usage	Specifies the usage type of the server.	R
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

RMON Commands

Command	Description	Mode*
rmon alarm	Configures alarm conditions.	GC
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	IC
rmon event	Configures an RMON event.	GC
rmon table-size	Configures the maximum RMON tables sizes.	GC
show rmon alarm	Displays alarm configurations.	UE
show rmon alarm-table	Displays the alarms summary table.	UE
show rmon collection history	Displays the requested group of statistics.	UE
show rmon events	Displays the RMON event table.	UE
show rmon history	Displays RMON Ethernet Statistics history.	UE
show rmon log	Displays the RMON logging table.	UE

show rmon statistics	Displays RMON Ethernet Statistics.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.*		

SNMP Commands

Command	Description	Mode*
show snmp	Displays the SNMP status.	PE
show snmp engineID	Displays the SNMP engine ID.	PE
show snmp filters	Displays the configuration of filters.	PE
show snmp groups	Displays the configuration of groups.	PE
show snmp users	Displays the configuration of users.	PE
show snmp views	Displays the configuration of views.	PE
snmp-server community	Sets up the community access string to permit access to SNMP protocol.	GC
snmp-server community-group	Maps SNMP v1 and v2 security models to the group name.	GC
snmp-server contact	Sets up a system contact (sysContact) string.	GC
snmp-server enable traps	Enables the switch to send SNMP traps or SNMP notifications.	GC
snmp-server engineID local	Specifies the Simple Network Management Protocol (SNMP) engine ID on the local switch.	GC
snmp-server filter	Creates or updates an SNMP server filter entry.	GC
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.	GC
snmp-server host	Specifies the recipient of SNMP notifications.	GC
snmp-server location	Sets the system location string.	GC
snmp-server trap authentication	Enables the switch to send SNMP traps when authentication failed.	GC
snmp-server v3-host	Specifies the recipient of SNMPv3 notifications.	GC
snmp-server user	Configures a new SNMP Version 3 user.	GC
snmp-server view	Creates or updates a Simple Network Management Protocol (SNMP) server view entry.	GC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.*		

Port Channel Commands

Command	Description	Mode*
channel-group	Associates a port with a port-channel.	IC
interface port-channel	Enters the interface configuration mode of a specific port-channel.	GC
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.	GC
hashing-mode	Sets the hashing algorithm on trunk ports.	IC (port-channel)
no hashing-mode	Sets the hashing algorithm on trunk ports to default (3).	IC (port-channel)
show interfaces port-channel	Displays port-channel information.	PE
show statistics port-channel	Displays port-channel statistics.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Spanning Tree Commands

Command	Description	Mode*
abort (mst)	Exits the MST configuration mode without applying configuration changes.	MC
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.	PE
exit (mst)	Exits the MST configuration mode and applies configuration changes.	MC
instance (mst)	Maps VLANs to an MST instance.	MC
name (mst)	Defines the MST configuration name.	MC
revision (mst)	Defines the configuration revision number.	MC
show (mst)	Displays the current or pending MST region configuration	MC
show spanning-tree	Displays spanning tree configuration.	PE
spanning tree	Enables spanning-tree functionality.	GC
spanning-tree bpdu	Defines the bridge protocol data unit (BPDU) handling when spanning tree is disabled on an interface.	GC
spanning-tree bpdu-protection	Enables BPDU protection on a switch.	GC
spanning-tree cost	Configures the spanning tree path cost for a port.	IC

Command	Description	Mode*
spanning-tree disable	Disables spanning tree on a specific port.	IC
spanning-tree forward-time	Configures the spanning tree bridge forward time.	GC
spanning-tree hello-time	Configures the spanning tree bridge Hello Time.	GC
spanning-tree link-type	Overrides the default link-type setting.	IC
spanning-tree max-age	Configures the spanning tree bridge maximum age.	GC
spanning-tree mode	Configures the spanning tree protocol.	GC
spanning-tree mst configuration	Enables configuring an MST region by entering the multiple spanning-tree (MST) mode.	GC
spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations.	IC
spanning-tree pathcost method	Configures the spanning tree default pathcost method	GC
spanning-tree mst max-hops	Configures the number of hops in an MST region before the BPDU is discarded and port information is aged out.	GC
spanning-tree mst port-priority	Configures port priority.	IC
spanning-tree mst priority	Configures the switch priority for the specified spanning tree instance.	GC
spanning-tree portfast	Enables PortFast mode.	IC
spanning-tree port-priority	Configures port priority.	IC
spanning-tree priority	Configures the spanning tree priority.	GC
spanning-tree root protection	Enables the root protection function on a switch.	IC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

SSH Commands

Command	Description	Mode*
crypto key generate dsa	Generates DSA key pairs for the switch.	GC
crypto key generate rsa	Generates RSA key pairs for the switch.	GC
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.	GC
ip ssh port	Specifies the port to be used by the SSH server.	GC
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.	GC
ip ssh server	Enables the switch to be configured from a SSH server connection.	GC

key-string	Manually specifies a SSH public key.	SK
show crypto key mypubkey	Displays its own SSH public keys stored on the switch.	PE
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the switch.	PE
show ip ssh	Displays the SSH server configuration.	PE
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	SP
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Syslog Commands

Command	Description	Mode*
clear logging	Clears messages from the internal logging buffer.	PE
clear logging file	Clears messages from the logging file.	PE
description	Describes the syslog server.	L
level	Specifies the importance level of syslog messages.	L
loggin cli-command	Enable CLI command logging	GC
logging	Logs messages to a syslog server	GC
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.	GC
logging buffered size	Changes the number of syslog messages stored in the internal buffer.	GC
logging console	Limits messages logged to the console based on severity.	GC
logging facility	Sets the facility of the logging messages.	GC
logging file	Limits syslog messages sent to the logging file based on severity.	GC
logging on	Controls error messages logging.	GC
port	Specifies the port number of syslog messages.	L
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	PE
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	PE
show syslog-servers	Displays the syslog servers settings.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

TACACS+ Commands

Command	Description	Mode*
key	Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server.	TC
port	Specifies a server port number.	TC
priority	Specifies the order in which servers are used.	TC
show tacacs	Displays TACACS+ server settings and statistics.	PE
tacacs-server host	Specifies a TACACS+ server host.	GC
tacacs-server key	Sets the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon.	GC
tacacs-server timeout	Sets the interval for which the switch waits for a server host to reply.	GC
timeout	Specifies the timeout value in seconds.	TC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Telnet Server Commands

Command	Description	Mode*
ip telnet server disable	Enables/disables the Telnet service on the switch.	GC
ip telnet port	Configures the Telnet service port number on the switch.	GC
show ip telnet	Displays the status of the Telnet server and the Telnet service port number.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

VLAN Commands

Command	Description	Mode*
dvlan-tunnel ethertype	Configures the EtherType for the interface.	GC
interface vlan	Enters the interface configuration (VLAN) mode.	GC
interface range vlan	Enters the interface configuration mode to configure multiple VLANs.	GC
mode dvlan-tunnel	Enables Double VLAN tunneling on the specified interface	IC

Command	Description	Mode*
name	Configures a name to a VLAN.	IC
protocol group	Attaches a *vlanid* to the protocol-based VLAN identified by *groupid*.	VLAN
protocol vlan group	Adds the physical unit/port interface to the protocol-based VLAN identified by *groupid*.	IC
protocol vlan group all	Adds all physical unit/port interfaces to the protocol-based VLAN identified by *groupid*.	GC
show dvlan-tunnel	Displays all interfaces enabled for Double VLAN Tunneling.	PE
show dvlan-tunnel interface	Displays detailed information about Double VLAN Tunneling for the specified interface.	PE
show interfaces switchport	Displays switchport configuration.	PE
show port protocol	Displays the Protocol-Based VLAN information for either the entire system or for the indicated group	PE
show switchport protected	Displays protected group/port information.	PE
show vlan	Displays VLAN information.	PE
show vlan association mac	Displays the VLAN associated with a specific configured MAC address.	PE
show vlan association subnet	Displays the VLAN associated with a specific configured IP subnet.	PE
switchport access vlan	Configures the VLAN ID when the interface is in access mode.	IC
switchport forbidden vlan	Forbids adding specific VLANs to a port.	IC
switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress.	IC
switchport general allowed vlan	Adds or removes VLANs from a port in General mode.	IC
switchport general ingress-filtering disable	Disables port ingress filtering.	IC
switchport general pvid	Configures the PVID when the interface is in general mode.	IC
switchport mode	Configures the VLAN membership mode of a port.	IC
switchport protected	Sets the port to Protected mode.	IC
switchport protected name	Configures a name for a protected group	GC
switchport trunk allowed vlan	Adds or removes VLANs from a port in general mode.	IC

Command	Description	Mode*
vlan	Creates a VLAN.	VLAN
vlan association mac	Associates a MAC address to a VLAN.	VLAN
vlan association subnet	Associates an IP subnet to a VLAN	VLAN
vlan database	Enters the VLAN database configuration mode.	GC
vlan makestatic	Changes a dynamically created VLAN to a static VLAN.	VLAN
vlan protocol group	Adds protocol-based VLAN groups to the system.	GC
vlan protocol group add protocol	Adds a protocol to the protocol-based VLAN identified by *groupid*.	GC
vlan protocol group remove	Removes the protocol-base VLAN group identified by *groupid*.	GC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Web Server Commands

Command	Description	Mode*
common-name	Specifies the common-name for the device.	CC
country	Specifies the country.	CC
crypto certificate generate	Generates a HTTPS certificate.	GC
crypto certificate import	Imports a certificate signed by the Certification Authority for HTTPS	PE
crypto certificate request	Generates and displays a certificate request for HTTPS	PE
duration	Specifies the duration in days.	CC
ip http port	Specifies the TCP port for use by a web browser to configure the switch.	GC
ip http server	Enables the switch to be configured from a browser.	GC
ip https certificate	Configures the active certificate for HTTPS	GC
ip https port	Configures a TCP port for use by a secure web browser to configure the switch.	GC
ip https server	Enables the switch to be configured from a secured browser.	GC
key-generate	Specifies the key-generate.	CC
location	Specifies the location or city name.	CC
organization-unit	Specifies the organization-unit or department name	CC

show crypto certificate mycertificate	Displays the SSL certificates of your switch.	PE
show ip http	Displays the HTTP server configuration.	PE
show ip https	Displays the HTTPS server configuration.	PE
state	Specifies the state or province name.	CC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Layer 3 Commands

ARP Commands

Command	Description	Mode*
arp	Creates an Address Resolution Protocol (ARP) entry.	GC
arp cachesize	Configures the maximum number of entries in the ARP cache.	GC
arp dynamicrenew	Enables the ARP component to automatically renew dynamic ARP entries when they age out.	GC
arp purge	Causes the specified IP address to be removed from the ARP cache.	PE
arp resptime	Configures the ARP request response timeout.	GC
arp retries	Configures the ARP count of maximum request for retries.	GC
arp timeout	Configures the ARP entry age-out time.	GC
clear arp-cache	Removes all ARP entries of type dynamic from the ARP cache.	PE
ip proxy-arp	Enables proxy ARP on a router interface.	IC
show arp	Displays the Address Resolution Protocol (ARP) cache.	PE
show arp brief	Displays the brief Address Resolution Protocol (ARP) table information.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

DHCP and BOOTP Relay Commands

Command	Description	Mode*
bootpdhcprelay cidridoptmode	Enables the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system.	GC
bootpdhcprelay enable	Enables the forwarding of relay requests for BootP/DHCP Relay on the system.	GC
bootpdhcprelay maxhopcount	Configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.	GC
bootpdhcprelay minwaittime	Configures the minimum wait time in seconds for BootP/DHCP Relay on the system.	GC
bootpdhcprelay serverip	Configures the server IP address for BootP/DHCP Relay on the system.	GC

Command	Description	Mode*
show bootpdhcprelay	Displays the BootP/DHCP Relay information.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.*		

DHCPv6 Commands

Command	Description	Mode*
clear ipv6 dhcp	Clears DHCPv6 statistics for all interfaces or for a specific interface.	PE
dns-server	Sets the ipv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server.	v6DP
domain-name	Sets the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server.	v6DP
ipv6 dhcp pool	Enters IPv6 DHCP Pool Configuration mode.	GC
ipv6 dhcp relay	Configures an interface for DHCPv6 relay functionality.	IC
ipv6 dhcp relay-agent-info-opt	Configures a number to represent the DHCPv6 Relay Agent Information Option.	GC
ipv6 dhcp relay-agent-info-remote-id-subopt	Configures a number to represent the DHCPv6 the “remote-id” sub-option.	GC
ipv6 dhcp server	Configures DHCPv6 server functionality on an interface.	IC
prefix-delegation	Defines Multiple IPv6 prefixes within a pool for distributing to specific DHCPv6 Prefix delegation clients.	v6DP
service dhcpv6	Enables DHCPv6 configuration on the router.	GC
show ipv6 dhcp	Displays the DHCPv6 server name and status.	PE
show ipv6 dhcp binding	Displays the configured DHCP pool.	PE
show ipv6 dhcp interface	Displays DHCPv6 information for all relevant interfaces or a specified interface.	UE
show ipv6 dhcp pool	Displays the configured DHCP pool.	PE
show ipv6 dhcp statistics	Displays the DHCPv6 server name and status.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.*		

DVMRP Commands

Command	Description	Mode*
ip dvmrp	Sets the administrative mode of DVMRP in the router to active.	GC IC
ip dvmrp metric	Configures the metric for an interface.	IC
ip dvmrp trapflags	Enables the DVMRP trap mode.	GC
show ip dvmrp	Displays the system-wide information for DVMRP.	PE
show ip dvmrp interface	Displays the interface information for DVMRP on the specified interface.	PE
show ip dvmrp neighbor	Displays the neighbor information for DVMRP.	PE
show ip dvmrp nexthop	Displays the next hop information on outgoing interfaces for routing multicast datagrams.	PE
show ip dvmrp prune	Displays the table that lists the router's upstream prune information.	PE
show ip dvmrp route	Displays the multicast routing information for DVMRP.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IGMP Commands

Command	Description	Mode*
ip igmp	Sets the administrative mode of IGMP in the system to active.	GC
ip igmp last-member-query-count	Sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.	IC
ip igmp last-member-query-interval	Configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.	IC
ip igmp query-interval	Configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.	IC
ip igmp query-max-response-time	Configures the maximum response time interval for the specified interface.	IC
ip igmp robustness	Configures the robustness that allows tuning of the interface.	IC

Command	Description	Mode*
ip igmp startup-query-count	Sets the number of queries sent out on startup - at intervals equal to the startup query interval for the interface.	IC
ip igmp startup-query-interval	Sets the interval between general queries sent at startup on the interface.	IC
ip igmp version	Configures the version of IGMP for an interface.	IC
show ip igmp	Displays system-wide IGMP information.	PE
show ip igmp groups	Displays the registered multicast groups on the interface.	PE
show ip igmp interface	Displays the IGMP information for the specified interface.	PE
show ip igmp interface membership	Displays the list of interfaces that have registered in the multicast group.	PE
show ip igmp interface stats	Displays the IGMP statistical information for the interface.	PE
ip igmp router-alert-optional	Sets IGMP to not require the Router-Alert field.	GC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IGMP Proxy Commands

Command	Description	Mode*
ip igmp-proxy	Enables the IGMP Proxy on the router.	IC
ip igmp-proxy reset-status	Resets the host interface status parameters of the IGMP Proxy router.	IC
ip igmp-proxy unsolicited-report-interval	Sets the unsolicited report interval for the IGMP Proxy router.	IC
show ip igmp-proxy	Displays a summary of the host interface status parameters.	PE
show ip igmp-proxy interface	Displays a detailed list of the host interface status parameters.	PE
show ip igmp-proxy groups	Displays a table of information about multicast groups that IGMP Proxy reported.	PE
show ip igmp-proxy groups detail	Displays complete information about multicast groups that IGMP Proxy has reported.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IP Routing Commands

Command	Description	Mode*
encapsulation	Configures the link layer encapsulation type for the packet.	IC
ip address	Configures an IP address on an interface.	IC
ip mtu	Sets the IP Maximum Transmission Unit (MTU) on a routing interface.	IC
ip netdirbcast	Enables the forwarding of network-directed broadcasts.	IC
ip route	Configures a static route. Use the no form of the command to delete the static route.	GC
ip route default	Configures the default route. Use the no form of the command to delete the default route.	GC
ip route distance	Sets the default distance (preference) for static routes.	GC
ip routing	Globally enables IPv4 routing on the router.	GC
routing	Enables IPv4 and IPv6 routing for an interface.	IC
show ip brief	Displays all the summary information of the IP.	PE
show ip interface	Displays all pertinent information about the IP interface.	PE
show ip protocols	Displays the parameters and current state of the active routing protocols.	PE
show ip route	Displays the routing table.	PE
show ip route preferences	Displays detailed information about the route preferences.	PE
show ip route summary	Shows the number of all routes, including best and non-best routes.	PE
show ip stats	Displays IP statistical information	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

IPv6 Routing Commands

Command	Description	Mode*
clear ipv6 neighbors	Clears all entries in the IPv6 neighbor table or an entry on a specific interface.	PE
clear ipv6 statistics	Clears IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces.	PE
ipv6 address	Configures an IPv6 address on an interface (including tunnel and loopback interfaces).	IC

Command	Description	Mode*
ipv6 enable	Enables IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address.	IC
ipv6 forwarding	Enables IPv6 forwarding on a router.	GC
ipv6 mtu	Sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface.	IC
ipv6 nd dad attempts	Sets the number of duplicate address detection probes transmitted while doing neighbor discovery.	IC
ipv6 nt managed-config-flag	Sets the "managed address configuration" flag in router advertisements.	IC
ipv6 nd ns-interval	Sets the interval between router advertisements for advertised neighbor solicitations.	IC
ipv6 nd other-config-flag	Sets the "other stateful configuration" flag in router advertisements sent from the interface.	IC
ipv6 nd prefix	Set the IPv6 prefixes to include in the router advertisement.	IC
ipv6 nd ra-interval	Sets the transmission interval between router advertisements.	IC
ipv6 nd ra-lifetime	Sets the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.	IC
ipv6 nd reachable-time	Sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.	IC
ipv6 nd suppress-ra	Suppresses router advertisement transmission on an interface.	IC
ipv6 route	Configures an IPv6 static route	GC
ipv6 route distance	Sets the default distance (preference) for static routes.	GC
ipv6 unicast-routing	Enables forwarding of IPv6 unicast datagrams.	GC
ping ipv6	Determines whether another computer is on the network.	PE
ping ipv6 interface	Determines whether another computer is on the network using **Interface** keyword.	PE
show ipv6 brief	Displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.	PE
show ipv6 interface	Shows the usability status of IPv6 interfaces.	PE
show ipv6 neighbors	Displays information about the IPv6 neighbors.	PE
show ipv6 route	Displays the IPv6 routing table.	PE

Command	Description	Mode*
show ipv6 route preference	Shows the preference value associated with the type of route.	PE
show ipv6 route summary	Displays a summary of the routing table.	PE
show ipv6 traffic	Shows traffic and statistics for IPv6 and ICMPv6.	UE
show ipv6 vlan	Displays IPv6 VLAN routing interface addresses.	PE
traceroute ipv6	Discovers the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Loopback Interface Commands

Command	Description	Mode*
interface loopback	Enters the Interface Loopback configuration mode.	GC
show interface loopback	Displays information about configured loopback interfaces.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Multicast Commands

Command	Description	Mode*
ip mcast boundary	Adds an administrative scope multicast boundary.	IC
ip multicast	Sets the administrative mode of the IP multicast forwarder in the router to active.	GC
ip multicast staticroute	Creates a static route which is used to perform RPF checking in multicast packet forwarding.	GC
ip multicast ttl-threshold	Applies a *ttlvalue* to a routing interface.	IC
mrinfo	Queries the neighbor information for a multicast-capable router specified by *ipaddr*.	PE
mstat	Finds the IP Multicast packet rate and loss information path from a source to a receiver.	PE
mtrace	Finds the IP Multicast path from a source to a receiver.	PE
no ip mcast mroute	Clears entries in the mroute table.	GC
show ip mcast	Displays the system-wide multicast information.	PE
show ip mcast boundary	Displays the system-wide multicast information.	PE

Command	Description	Mode*
show ip mcast interface	Displays the multicast information for the specified interface.	PE
show ip mcast mroute	Displays a summary or all the details of the multicast table.	PE
show ip mcast mroute group	Displays the multicast configuration settings of entries in the multicast mroute table.	PE
show ip mcast mroute source	Displays the multicast configuration settings of entries in the multicast mroute table.	PE
show ip mcast mroute static	Displays all the static routes configured in the static mcast table.	PE
show mrinfo	Displays neighbor information of a multicast-capable router.	PE
show mstat	Displays the results of packet rate and loss information from the results buffer pool of the router.	PE
show mtrace	Displays results of multicast trace path from the results buffer pool of the router	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

OSPF Commands

Command	Description	Mode*
area default-cost	Configures the monetary default cost for the stub area.	ROSPF
area nssa	Configures the specified area ID to function as an NSSA.	ROSPF
area nssa default-info-originate	Configures the metric value and type for the default route advertised into the NSSA.	ROSPF
area nssa no-redistribute	Configures the NSSA Area Border router (ABR) so that learned external routes are not redistributed to the NSSA.	ROSPF
area nssa no-summary	Configures the NSSA so that summary LSAs are not advertised into the NSSA.	ROSPF
area nssa translator-role	Configures the translator role of the NSSA.	ROSPF
area nssa translator-stab-intv	Configures the translator stability interval of the NSSA.	ROSPF
area range	Creates a specified area range for a specified NSSA.	ROSPF
area stub	Creates a stub area for the specified area ID.	ROSPF
area stub no-summary	Prevents Summary LSAs from being advertised into the NSSA.	ROSPF

Command	Description	Mode*
area virtual-link	Creates the OSPF virtual interface for the specified area-id and neighbor router.	ROSPF
area virtual-link authentication	Configures the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID.	ROSPF
area virtual-link dead-interval	Configures the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router.	ROSPF
area virtual-link hello-interval	Configures the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
area virtual-link retransmit-interval	Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
area virtual-link transmit-delay	Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
default-information originate	Controls the advertisement of default routes.	ROSPF
default-metric	Sets a default for the metric of distributed routes.	ROSPF
distance ospf	Sets the route preference value of OSPF in the router.	ROSPF
distribute-list out	Specifies the access list to filter routes received from the source protocol.	ROSPF
enable	Resets the default administrative mode of OSPF in the router (active).	ROSPF
exit-overflow-interval	Configures the exit overflow interval for OSPF.	ROSPF
external-lsdb-limit	Configures the external LSDB limit for OSPF.	ROSPF
ip ospf	Enables OSPF on a router interface	IC
ip ospf areaid	Sets the OSPF area to which the specified router interface belongs.	IC
ip ospf authentication	Sets the OSPF Authentication Type and Key for the specified interface.	IC
ip ospf cost	Configures the cost on an OSPF interface.	IC
ip ospf dead-interval	Sets the OSPF dead interval for the specified interface.	IC
ip ospf hello-interval	Sets the OSPF hello interval for the specified interface.	IC
ip ospf mtu-ignore	Disables OSPF maximum transmission unit (MTU) mismatch detection.	IC
ip ospf priority	Sets the OSPF priority for the specified router interface.	IC

Command	Description	Mode*
ip ospf retransmit-interval	Sets the OSPF retransmit Interval for the specified interface.	IC
ip ospf transmit-delay	Sets the OSPF Transit Delay for the specified interface.	IC
maximum-paths	Sets the number of paths that OSPF can report for a given destination.	ROSPF
redistribute	Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.	ROSPF
router-id	Sets a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.	ROSPF
router ospf	Enters Router OSPF mode.	GC
show ip ospf	Displays information relevant to the OSPF router.	PE
show ip ospf abr	Displays the internal OSPF routing table entries to Area Border Routers (ABR).	PE UE
show ip ospf area	Displays information about the identified OSPF area.	PE
show ip ospf asbr	Displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR).	PE UE
show ip ospf database	Displays information about the link state database when OSPF is enabled.	PE
show ip ospf database database-summary	Displays the number of each type of LSA in the database for each area and for the router.	PE
show ip ospf interface	Displays the information for the IFO object or virtual interface tables.	PE
show ip ospf interface brief	Displays brief information for the IFO object or virtual interface tables.	PE
show ip ospf interface stats	Displays the statistics for a specific interface.	PE
show ip ospf neighbor	Displays information about OSPF neighbors.	PE
show ip ospf range	Displays information about the area ranges for the specified area-id.	PE
show ip ospf statistics	Displays information about recent Shortest Path First (SPF) calculations.	PE UE
show ip ospf stub table	Displays the OSPF stub table.	PE
show ip ospf virtual-link	Displays the OSPF Virtual Interface information for a specific area and neighbor.	PE
show ip ospf virtual-link brief	Displays the OSPF Virtual Interface information for all areas in the system.	PE
timers spf	Configures the SPF delay and hold time.	ROSPF

Command	Description	Mode*
trapflags	Enables OSPF traps.	ROSPF
1583compatibility	Enables OSPF 1583 compatibility.	ROSPF
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

OSPFv3 Commands

Command	Description	Mode*
area default-cost	Configures the monetary default cost for the stub area.	ROSV3
area nssa	Configures the specified areaid to function as an NSSA.	ROSV3
area nssa default-info-originate	Configures the metric value and type for the default route advertised into the NSSA.	ROSV3
area nssa no-redistribute	Configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.	ROSV3
area nssa no-summary	Configures the NSSA so that summary LSAs are not advertised into the NSSA.	ROSV3
area nssa translator-role	Configures the translator role of the NSSA.	ROSV3
area nssa translator-stab-intv	Configures the translator stability interval of the NSSA.	ROSV3
area range	Creates an area range for a specified NSSA.	ROSV3
area stub	Creates a stub area for the specified area ID.	ROSV3
area stub no-summary	Disables the import of Summary LSAs for the stub area identified by *areaid*.	ROSV3
area virtual-link	Creates the OSPF virtual interface for the specified *areaid* and *neighbor*.	ROSV3
area virtual-link dead-interval	Configures the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.	ROSV3
area virtual-link hello-interval	Configures the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.	ROSV3
area virtual-link retransmit-interval	Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.	ROSV3
area virtual-link transmit-delay	Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.	ROSV3
default-information originate	Controls the advertisement of default routes.	ROSV3

Command	Description	Mode*
default-metric	Sets a default for the metric of distributed routes.	ROSV3
distance ospf	Sets the route preference value of OSPF in the router.	ROSV3
enable	Resets the default administrative mode of OSPF in the router (active).	ROSV3
exit-overflow-interval	Configures the exit overflow interval for OSPF.	ROSV3
external-lsdb-limit	Configures the external LSDB limit for OSPF.	ROSV3
ipv6 ospf	Enables OSPF on a router interface or loopback interface.	IC
ipv6 ospf areaid	Sets the OSPF area to which the specified router interface belongs.	IC
ipv6 ospf cost	Configures the cost on an OSPF interface.	IC
ipv6 ospf dead-interval	Sets the OSPF dead interval for the specified interface.	IC
ipv6 ospf hello-interval	Sets the OSPF hello interval for the specified interface.	IC
ipv6 ospf mtu-ignore	Disables OSPF maximum transmission unit (MTU) mismatch detection.	IC
ipv6 ospf network	Changes the default OSPF network type for the interface.	IC
ipv6 ospf priority	Sets the OSPF priority for the specified router interface.	IC
ipv6 ospf retransmit-interval	Sets the OSPF retransmit interval for the specified interface.	IC
ipv6 ospf transmit-delay	Sets the OSPF Transmit Delay for the specified interface.	IC
ipv6 router ospf	Enters Router OSPFv3 Configuration mode.	GC
maximum-paths	Sets the number of paths that OSPF can report for a given destination.	ROSV3
redistribute	Configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.	ROSV3
router-id	Sets a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.	ROSV3
show ipv6 ospf	Displays information relevant to the OSPF router.	PE
show ipv6 ospf abr	Displays the internal OSPFv3 routes to reach Area Border Routers (ABR).	PE UE
show ipv6 ospf area	Displays information about the area.	PE
show ipv6 ospf asbr	Displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR).	PE UE
show ipv6 ospf database	Displays information about the link state database when OSPFv3 is enabled.	PE

Command	Description	Mode*
show ipv6 ospf database database-summary	Displays the number of each type of LSA in the database and the total number of LSAs in the database.	PE
show ipv6 ospf interface	Display the information for the IFO object or virtual interface tables.	PE
show ipv6 ospf interface brief	Displays brief information for the IFO object or virtual interface tables.	PE
show ipv6 ospf interface stats	Displays the statistics for a specific interface.	UE
show ipv6 ospf interface vlan	Displays OSPFv3 configuration and status information for a specific vlan	PE
show ipv6 ospf neighbor	Displays information about OSPF neighbors.	PE
show ipv6 ospf range	Displays information about the area ranges for the specified area identifier.	PE
show ipv6 ospf stub table	Displays the OSPF stub table.	PE
show ipv6 ospf virtual-link	Displays the OSPF Virtual Interface information for a specific area and neighbor.	PE
show ipv6 ospf virtual-link brief	Displays the OSPFV3 Virtual Interface information for all areas in the system.	PE
trapflags	Enables OSPF traps	ROSV3
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

PIM-DM Commands

Command	Description	Mode*
ip pimdm	Enables the administrative mode of PIM-DM in the router.	GC
ip pimdm mode	Sets administrative mode of PIM-DM on an interface to enabled.	IC
ip pimdm query-interval	Configures the transmission frequency of hello messages between PIM enabled neighbors.	IC
show ip pimdm	Displays system-wide information for PIM-DM.	PE
show ip pimdm interface	Displays interface information for PIM-DM on the specified interface.	PE
show ip pimdm interface stats	Displays the statistical information for PIM-DM on the specified interface.	UE
show ip pimdm neighbor	Displays the neighbor information for PIM-DM on the specified interface.	PE

Command	Description	Mode*
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

PIM-SM Commands

Command	Description	Mode*
ip pimsm	Sets administrative mode of PIM-SM multicast routing across the router to enabled.	GC
ip pimsm cbsrhasmasklength	Configures the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface.	IC
ip pimsm cbsrpreference	Configures the CBSR preference for a particular PIM-SM interface.	IC
ip pimsm crppreference	Configures the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface.	IC
ip pimsm message-interval	Configures the global join/prune interval for PIM-SM router.	GC
ip pimsm mode	Sets to enabled the administrative mode of PIM-SM multicast routing on a routing interface.	IC
ip pimsm query-interval	Configures the transmission frequency of hello messages in seconds between PIM enabled neighbors.	IC
ip pimsm register-rate-limit	Sets the Register Threshold rate for the RP (Rendezvous Point) router to switch to the shortest path.	GC
ip pimsm spt-threshold	Configures the threshold rate for the RP router to switch to the shortest path.	GC
ip pimsm staticrp	Creates RP IP address for the PIM-SM router.	GC
ip pim-trapflags	Enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode (DM).	GC
show ip pimsm	Displays the system-wide information for PIM-SM.	PE
show ip pimsm componenttable	Displays the table containing objects specific to a PIM domain.	PE
show ip pimsm interface	Displays interface information for PIM-SM on the specified interface.	PE
show ip pimsm interface stats	Displays the statistical information for PIM-SM on the specified interface.	UE
show ip pimsm neighbor	Displays neighbor information for PIM-SM on the specified interface.	PE

Command	Description	Mode*
show ip pimsm rp	Displays PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific group address or group mask provided in the command.	PE
show ip pimsm rphash	Displays the RP router being selected from the set of active RP routers.	PE
show ip pimsm staticrp	Displays the static RP information for the PIM-SM router.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Router Discovery Protocol Commands

Command	Description	Mode*
ip irdp	Enables Router Discovery on an interface.	IC
ip irdp address	Configures the address that the interface uses to send the router discovery advertisements.	IC
ip irdp holdtime	Configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.	IC
ip irdp maxadvertinterval	Configures the maximum time, in seconds, allowed between sending router advertisements from the interface.	IC
ip irdp minadvertinterval	Configures the minimum time, in seconds, allowed between sending router advertisements from the interface.	IC
ip irdp preference	Configures the preference of the address as a default router address relative to other router addresses on the same subnet.	IC
show ip irdp	Displays the router discovery information for all interfaces, or for a specified interface.	PE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Routing Information Protocol (RIP) Commands

Command	Description	Mode*
auto-summary	Enables the RIP auto-summarization mode.	RIP
default-information originate	Controls the advertisement of default routes.	RIP
default-metric	Sets a default for the metric of distributed routes.	RIP
distance rip	Sets the route preference value of RIP in the router.	RIP

Command	Description	Mode*
distribute-list out	Specifies the access list to filter routes received from the source protocol.	RIP
enable	Resets the default administrative mode of RIP in the router (active).	RIP
hostroutesaccept	Enables the RIP hostroutesaccept mode.	RIP
ip rip	Enables RIP on a router interface.	IC
ip rip authentication	Sets the RIP Version 2 Authentication Type and Key for the specified interface.	IC
ip rip receive version	Configures the interface to allow RIP control packets of the specified version(s) to be received.	IC
ip rip send version	Configures the interface to allow RIP control packets of the specified version to be sent.	IC
redistribute	Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.	ROSPF
router rip	Enters Router RIP mode.	GC
show ip rip	Displays information relevant to the RIP router.	PE
show ip rip interface	Displays information related to a particular RIP interface.	PE
show ip rip interface brief	Displays general information for each RIP interface.	PE
split-horizon	Sets the RIP split horizon mode.	RIP
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Tunnel Interface Commands

Command	Description	Mode*
interface tunnel	Enables the interface configuration mode for a tunnel.	GC
show interface tunnel	Displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.	PE
tunnel destination	Specifies the destination transport address of the tunnel.	IC
tunnel mode ipv6ip	Specifies the mode of the tunnel.	IC
tunnel source	Specifies the source transport address of the tunnel, either explicitly or by reference to an interface.	IC
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Virtual LAN Routing Commands

Command	Description	Mode*
show ip vlan	Displays the VLAN routing information for all VLANs with routing enabled.	PE
vlan routing	Creates routing on a VLAN	VLAN
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

Virtual Router Redundancy Commands

Command	Description	Mode*
ip vrrp	Enables the administrative mode of VRRP for the router.	GC
ip vrrp authentication	Sets the authorization details value for the virtual router configured on a specified interface.	IC
ip vrrp ip	Sets the virtual router IP address value for an interface.	IC
ip vrrp mode	Enables the virtual router configured on an interface. Enabling the status field starts a virtual router.	IC
ip vrrp preempt	Sets the preemption mode value for the virtual router configured on a specified interface.	IC
ip vrrp priority	Sets the priority value for the virtual router configured on a specified interface.	IC
ip vrrp timers advertise	Sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.	IC
show ip vrrp	Displays whether VRRP functionality is enabled or disabled on the switch.	PE
show ip vrrp interface	Displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.	PE
show ip vrrp interface brief	Displays information about each virtual router configured on the switch.	PE
show ip vrrp interface stats	Displays the statistical information about each virtual router configured on the switch.	UE
***NOTE:** For the meaning of each Mode abbreviation, see *Mode Types* on page 4.		

2

Using the CLI

This chapter describes the basics of entering and editing the Dell PowerConnect 62xx Series Command Line Interface (CLI) commands and defines the command hierarchy. It also explains how to activate the CLI and implement its major functions.

Entering and Editing CLI Commands

A CLI command is a series of keywords and arguments. Keywords identify a command and arguments specify configuration parameters. For example, in the command **show interfaces status ethernet** *1/g5*, **show**, **interfaces** and **status** are keywords; **ethernet** is an argument that specifies the interface type, and *1/g5* specifies the unit/port.

When working with the CLI, the command options are not displayed. The command is not selected by a menu but is entered manually. To see what commands are available in each mode or within an Interface Configuration, the CLI provides a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request context-sensitive help is the <?> key.

Two instances where the help information can be displayed are:

- **Keyword lookup**—The <?> key is entered in place of a command. A list of all valid commands and corresponding help messages is displayed.
- **Partial keyword lookup**—A command is incomplete and the <?> key is entered in place of a parameter. The matched parameters for this command are displayed.

The following features and conventions are applicable to CLI command entry and editing:

- History Buffer
- Negating Commands
- Show Command
- Command Completion
- Short Form Commands
- Keyboard Shortcuts
- Operating on Multiple Objects (Range)

- Command Scripting
- CLI Command Notation Conventions
- Interface Naming Conventions

History Buffer

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

Keyword	Source or Destination
Up-arrow key <Ctrl>+<P>	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key <Ctrl>+<N>	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence recalls more recent commands in succession.

By default, the history buffer system is enabled, but it can be disabled at any time. The standard number of 10 stored commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see the **history-size** command in the Line command mode chapter of this guide.

Negating Commands

For many commands, the prefix keyword **no** is entered to cancel the effect of a command or reset the configuration to the default value. All configuration commands have this capability. This guide describes the negation effect for all commands to which it applies.

Show Command

The **show** command executes in the User Executive (EXEC) and Privileged Executive (EXEC) modes.

Command Completion

CLI can complete partially entered commands when the user presses the <tab> or <space> key. If a command entered is not complete, is not valid, or if some parameters of the command are not valid or missing, an error message is displayed to assist in entering the correct command. By pressing the <tab> key, an incomplete command is changed into a complete command. If the characters already entered are not enough for the system to identify a single matching command, the <?>key displays the available commands matching the characters already entered.

Short Form Commands

The CLI supports the short forms of all commands. As long as it is possible to recognize the entered command unambiguously, the CLI accepts the short form of the command as if the user typed the full command.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The **help** command, when used in the User EXEC and Privileged EXEC modes, displays the keyboard short cuts.

The following table contains the CLI shortcuts displayed by the **help** command.

Keyboard Key	Description
<Delete, Backspace>	Delete previous character
<Ctrl>+<A>	Go to beginning of line
<Ctrl>+<E>	Go to end of line
<Ctrl>+<F>	Go forward one character
<Ctrl>+<B>	Go backward one character
<Ctrl>+<D>	Delete current character
<Ctrl>+<U,X>	Delete to beginning of line
<Ctrl>+<K>	Delete to the end of the line.
<Ctrl>+<W>	Delete previous word
<Ctrl>+<T>	Transpose previous character
<Ctrl>+<P>	Go to previous line history buffer
<Ctrl>+<R>	Rewrites or pastes the line
<Ctrl>+<N>	Go to next line in history buffer
<Ctrl>+<Y>	Print last deleted character
<Ctrl>+<Q>	Enables serial flow
<Ctrl>+<S>	Disables serial flow
<Ctrl>+<Z>	Return to root command prompt
<Tab, SPACE>	Command-line completion
end	Return to the root command prompt
exit	Go to next lower command prompt
<?>	List choices

Operating on Multiple Objects (Range)

The CLI allows the user to operate on the set of objects at the same time. The guidelines are as follows for range operation:

- Operations on objects with four or more instances support the range operation.
- The **range** key word is used to identify the range of objects on which to operate.
- The range may be specified in the following manner:

  (*#-#*) — a range from a particular instance to another instance (inclusive). For example, 1/g1-g10 indicates that the operation applies to the gigabit Ethernet ports 1 to 10 on unit 1.

  (*#, #, #*) — a list of non-consecutive instances. For example, (1/g1, 1/g3,1/g5) indicates that the operation applies to the gigabit Ethernet ports 1, 3, and 5 on unit 1.

  (*#, #-#, #*) — ranges and non-consecutive instances listed together. For example, (1/g1, 1/g3-g5, 1/g7) indicates that the operation applies to the gigabit Ethernet ports 1, 7, and 3 to 5 on unit 1.

NOTE: Each # must be a fully qualified port identifier, that is, type<unit>/<port_type><port_number>, where unit is 1-12, port_type is g or xg and port_number is 1-24 or 1-48 in the case of port_type g and 1-4 for port_type xg. The following formats are allowed:(*#-#,#*), (*#,#-#,#*), (*#,#-#,#-#,#*). For LAG, use "*interface range port-channel 1-18*".

- When operating on a range of objects, the CLI implementation hides the parameters that may not be configured in a range (for example, parameters that must be uniquely configured for each instance).
- The CLI uses best effort when operating on a list of objects. If the user requests an operation on a list of objects, the CLI attempts to execute the operation on as many objects in the list as possible even if failure occurs for some of the items in the list. The CLI provides the user with a detailed list of all failures, listing the objects and the reasons for the failures.
- Some parameters must be configured individually for each port or interface.

Command Scripting

The CLI can be used as a programmable management interface. To facilitate this function, any command line starting with the <!> character is treated as a comment line and ignored by the CLI. Also, the CLI allows the user to disable session timeouts.

CLI Command Notation Conventions

When entering commands there are certain command-entry notations which apply to all commands. The following table describes these conventions as they are used in syntax definitions.

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry.
{ }	In a command line inclusive brackets indicate a selection of compulsory parameters separated by the |character. One option must be selected. For example: **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic	Indicates a variable.
<Enter>	Any individual key on the keyboard.
<Ctrl>+<F4>	Any combination of keys pressed simultaneously on the keyboard.
`Screen Display`	Indicates system messages and prompts appearing on the console.
all	Indicates a literal parameter, entered into the command as it is.

Interface Naming Conventions

The conventions for naming interfaces in CLI commands are as follows:

- Unit#/Interface ID—each interface is identified by the *Unit#* followed by a </> symbol and then the *Interface ID*. For example, *2/g10* identifies the gigabit port 10 within the second unit.
- Unit#—the unit number is used only in a stacking solution where a number of switches are stacked to form a virtual switch. In this case, the *Unit #* identifies the physical switch identifier within the stack.
- Interface ID—is formed by the interface type followed by the interface number. For example, *2/g10* identifies the gigabit port 10 on the second unit; *1/g1* identifies the fast Ethernet port 1 on the first unit within the stack.
- Interface Types—the following interface types are defined. *g* stands for gigabit Ethernet port (for example, *g2* is the gigabit port 2). *xg* stands for 10 Gigabit Ethernet port (for example, xg2 is the 10 gigabit Ethernet port 2).

CLI Command Modes

Since the set of CLI commands is very large, the CLI is structured as a command-tree hierarchy, where related command sets are assigned to command modes for easier access. At each level, only the commands related to that level are available to the user and only those commands are shown in the context sensitive help for that level.

In this guide, commands are organized in two separate categories: Data Link Layer commands and Network Layer commands. The Data Link Layer (Layer 2) describes the logical organization of data bits transmitted on a particular medium. This layer defines the framing, addressing and checksumming of Ethernet packets. The Network Layer (Layer 3) describes how a series of exchanges over various data links can deliver data between any two nodes in a network. This layer defines the addressing and routing structure of the Internet.

Commands that cause specific actions to be taken immediately by the system and do not directly affect the system configurations are defined at the top of the command tree. For example, commands for rebooting the system or for downloading or backing up the system configuration files are placed at the top of the hierarchy tree.

Commands that result in configuration changes to the switch are grouped in a Configuration sub tree.

There are levels beneath the Configuration mode for further grouping of commands. The system prompt reflects these sub-Configuration modes.

All the parameters are provided with reasonable defaults where possible.

When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands is available in this mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged EXEC mode provides access to commands that can not be executed in the User EXEC mode and permits access to the switch Configuration mode.

The Global Configuration mode manages switch configuration on a global level. For specific interface configurations, command modes exist at a sub-level.

Entering a <?> at the system prompt displays a list of commands available for that particular command mode. A specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: User EXEC mode, Privileged EXEC mode, Global Configuration mode, and Interface Configuration and other specific configuration modes.

User EXEC Mode

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

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

```
console>
```

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

Privileged EXEC Mode

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

Privileged users enter into the Privileged EXEC mode from User EXEC mode, where the following prompt is displayed.

```
console#
```

Global Configuration Mode

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

```
console(config)#
```

Interface and Other Specific Configuration Modes

Interface configuration modes are used to modify specific interface operations. The following are the Interface Configuration and other specific configuration modes:

- **MST—**The Global Configuration mode command **spanning-tree mst configuration** is used to enter into the Multiple Spanning Tree configuration mode.
- **Line Interface**—Contains commands to configure the management connections. These include commands such as line speed and timeout settings. The Global Configuration mode command **line** is used to enter the Line Interface mode.
- **VLAN Database**—Contains commands to create a VLAN as a whole. The Global Configuration mode command **vlan database** is used to enter the VLAN Database mode.
- **Router OSPF Configuration** – Global configuration mode command **router ospf** is used to enter into the Router OSPF Configuration mode.
- **Router RIP Configuration** – Global configuration mode command **router rip** is used to enter into the Router RIP Configuration mode.
- **Router OSPFv3 Configuration** – Global configuration mode command **ipv6 router ospf** is used to enter into the Router OSPFv3 Configuration mode.
- **IPv6 DHCP Pool Mode**– Global configuration mode command **ipv6 dhcp pool** is used to enter into the IPv6 DHCP Pool mode.
- **Management Access List**—Contains commands to define management access administration lists. The Global Configuration mode command **management access-list** is used to enter the Management Access List configuration mode.

- **Policy-map**—Use the **policy-map** command to access the QoS policy map configuration mode to configure the QoS policy map.
- **Policy Class**—Use the **class** command to access the QoS Policy-class mode to attach or remove a diffserv class from a policy and to configure the QoS policy class.
- **Class-Map—**This mode consists of class creation/deletion and matching commands. The class matching commands specify layer 2, layer 3 and general match criteria. Use the class-map class-map-name commands to access the QoS Class Map Configuration mode to configure QoS class maps.
- **Stack**—Use the stack command to access the Stack Configuration Mode.
- **Ethernet**—Contains commands to manage Ethernet port configuration. The Global Configuration mode command **interface ethernet** enters the Interface Configuration mode to configure an Ethernet interface.
- **Port Channel**—Contains commands to configure port-channels, i.e., 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 Global Configuration mode command **interface port-channel** is used to enter the Port Channel mode.
- **Tunnel**-Contains commands to manage tunnel interfaces. The Global Configuration mode command interface tunnel enters the Tunnel Configuration mode to configure an tunnel type interface.
- **Loopback**-Contains commands to manage loopback interfaces. The Global Configuration mode command interface loopback enters the Loopback Configuration mode to configure an loopback type interface.
- **SSH Public Key-chain**—Contains commands to manually specify other switch SSH public keys. The Global Configuration mode command **crypto key pub-key chain ssh** is used to enter the SSH Public Key-**chain** configuration mode.
- **SSH Public Key-string**—Contains commands to manually specify the SSH Public-key of a remote SSH Client. The SSH Public-Key Chain Configuration mode command **user-key** command is used to enter the SSH Public-Key Configuration mode.
- **MAC Access-List**—Configures conditions required to allow traffic based on MAC addresses. The Global Configuration mode command **mac-access-list** is used to enter the MAC Access-List configuration mode.
- **TACACS**— Configures the parameters for the TACACS server.
- **Radius**— Configures the parameters for the RADIUS server.
- **SNMP Host Configuration**— Configures the parameters for the SNMP server host.
- **SNMP v3 Host Configuration**—Configures the parameters for the SNMP v3 server host.
- **SNMP Community Configuration**—Configures the parameters for the SNMP server community.

- **Crypto Certificate Request**— Configures the parameters for crypto certificate request.
- **Crypto Certificate Generation**—Configures the parameters for crypto certificate generate.
- **Logging**—Configures the parameters for syslog log server.

Identifying the Switch and Command Mode from the System Prompt

The system prompt provides the user with the name of the switch (hostname) and identifies the command mode. The following is a formal description of the system command prompt:

[*device name*][([*command mode*-[*object*]])][**#|>**]

[*device name*]— is the name of the managed switch, which is typically the user-configured hostname established by the **hostname** command.

[*command mode*]—is the current configuration mode and is omitted for the top configuration levels.

[*object*]—indicates specific object or range of objects within the configuration mode.

For example, if the current configuration mode is config-if and the object being operated on is gigabit ethernet 1 on unit 1, the prompt displays the object type and unit (for example, 1/g1).

[**# | >**]—The # sign is used to indicate that the system is in the Privileged EXEC mode. The > symbol indicates that the system is in the User EXEC mode, which is a read-only mode in which the system does not allow configuration.

Navigating CLI Command Modes

The following table describes how to navigate through the CLI Command Mode hierarchy.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
User EXEC	The user is automatically in User EXEC mode unless the user is defined as a privileged user.	`console>`	logout
Privileged EXEC	Use the **enable** command to enter into this mode. This mode is password protected.	`console#`	Use the **exit** command, or press <Ctrl>+<Z> to return to the User EXEC mode.
Global Configuration	From Privileged EXEC mode, use the **configure** command.	`console(config)#`	Use the **exit** command, or press <Ctrl>+<Z> to return to the Privileged EXEC mode.
Line Interface	From Global Configuration mode, use the **line** command.	`console(config-line)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Management Access-List	From Global Configuration mode, use the **management access-list** command.	`console(config-macal)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Policy-Class-Map	From Global Configuration mode, use the **policy-map class** command.	`console(config-policy-classmap)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Class-Map	From Global Configuration mode, use the **class-map** command.	`console(config-classmap)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
MAC Access List	From Global Configuration mode, use the **mac access-list** command.	`console(config-mac-access-list)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
SSH Public Key-Chain	From Global Configuration mode, use the **crypto key pubkey-chain ssh** command.	`console(config-pubkey-chain)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
SSH Public Key String	From the SSH Public Key- Chain mode, use the **user-key** <*user name* > {**rsa**|**dsa**} command.	`console(config-pubkey-key)#`	To return to the SSH Public key-chain mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
TACACS	From Global Configuration mode, use the **tacacs-server host** command.	`console(tacacs)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Radius	From Global Configuration mode, use the **radius-server host** command.	`console(config-radius)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
SNMP Host Configuration	From Global Configuration mode, use the **snmp-server** command.	`console(config-snmp)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
SNMP v3 Host Configuration	From Global Configuration mode, use the **snmp-server v3-host** command.	`console(config-snmp)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
SNMP Community Configuration	From Global Configuration mode, use the **snmp-server community** command.	`console(config-snmp)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode
Crypto Certificate Generation	From Global Configuration mode, use the **crypto certificate** *number* **generate** command.	`console(config-crypto-cert)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Crypto Certificate Request	From Privileged EXEC mode, use the **crypto certificate** *number* **request** command.	`console(config-crypto-cert)#`	To exit to Privileged EXEC mode, use the **exit** command, or press <Ctrl>+<Z>.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Stack	From Global Configuration mode, use the **stack** command.	`console(config-stack)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Logging	From Global Configuration mode, use the **logging** command.	`console(config-logging)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
MST	From Global Configuration mode, use the **spanning-tree mst configuration** command.	`console(config-mst)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
VLAN Config	From Global Configuration mode, use the **vlan database** command.	`console(config-vlan)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Router OSPF Conf	From Global Configuration mode, use the **router ospf** command.	`console(config-router)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode
Router RIP Config	From Global Configuration mode, use the **router rip** command.	`console(config-router)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Router OSPFv3 Config	From Global Configuration mode, use the **ipv6 router ospf** command.	`console(config-rtr)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode
IPv6 DHCP Pool Mode	From Global Configuration mode, use the **ipv6 dhcp pool** command.	`console(config-dhcp6s-pool)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode
Interface Configuration Modes			
Ethernet	From Global Configuration mode, use the **interface ethernet** command.	`console (config-if-n/gn` **or** `n/xgn)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Port Channel	From Global Configuration mode, use the **interface port-channel** command.	`console (config-if-chn)#`	To exit to Global Configuration mode, use the **exit** command, or <Ctrl>+<Z> to Privileged EXEC mode.
VLAN	From Global Configuration mode, use the **interface vlan** command.	`console(config-if-vlann)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Tunnel	From Global Configuration mode, use the **interface tunnel command.**	`console(config-tunneln)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.
Loopback	From Global configuration mode, use the **interface loopback** command.	`console(config-loopbackn)#`	To exit to Global Configuration mode, use the **exit** command, or press <Ctrl>+<Z> to Privileged EXEC mode.

Starting the CLI

To begin running the CLI, perform the following steps:

NOTE: This procedure is for use on the console line only.

NOTE: The Easy Setup Wizard is available only when the system is in default state with no user configuration saved previously.

1. Start the switch and wait until the startup procedure is complete and the User EXEC mode is entered. The prompt *console*> is displayed.
2. Configure the switch using the Easy Setup Wizard and enter the necessary commands to complete the required tasks.
3. When finished, exit the session with the **quit** or **exit** command.

The switch can be managed over a direct connection to the switch console port or through a Telnet connection. If access is through a Telnet connection, the switch must have a defined IP address, corresponding management access granted, and a connection to the network .

Easy Setup Wizard

The Easy Setup Wizard guides the user in the basic initial configuration of a newly installed switch so that it can be immediately deployed and functional in its basic operation and be completely manageable through the Web, CLI and the remote Dell Network Manager. After initial setup, the user may enter to the system to set up more advanced configurations.

By default the switch is shipped from the factory with an IP address of 192.168.2.1 but the Easy Setup Wizard provides the opportunity to customize the IP address. Also the system is set up with default management VLAN ID=1. The initial activation must be done using the serial interface since, without a unique IP address, the user can not access the other management interfaces.

The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the setup. The user may return to add users later. The initial account is given the highest privilege level (level 15).
- Enables CLI login and HTTP access to use the local authentication setting only, which allows user account access via these management interfaces. The user may return later to configure Radius or TACACS+.
- Sets up the IP address for the management VLAN or enables support for DHCP to configure the management IP address dynamically.
- Sets up the SNMP community string to be used by the SNMP manager. The user may choose to skip this step if SNMP management is not used. If it is configured, the default access level is set to the highest available access for the SNMP management interface. The user may return later to add to the community string or reconfigure the access level of the community string. Initially only SNMPv1/2c will be activated. SNMPv3 is disabled until the user returns to configure security access for SNMPv3 (for example, engine ID, view, and so on). The SNMP community string may include spaces. The wizard requires the use of quotation marks when the user wants to enter spaces in the community string. Although spaces are allowed in the community string, their use is discouraged. The default community string contains no spaces.
- Allows the user to specify the management server IP or permit SNMP access from all IP addresses.
- Sets up the default gateway IP address.

If the user chooses not to use the wizard initially, the session defaults to the CLI mode with a warning to refer the documentation. During a subsequent login, the user may again elect not to run the setup wizard. Once the wizard has established configuration, however, the wizard is presented only if the user resets the switch to the factory default settings. While the wizard is running, the system does not display any unsolicited or unrelated status messages. For example, the system does not display event notification or system status messages.

After completing the wizard, the user is given a chance to save his configuration and continue to the CLI. If the user chooses to discard his configuration, any restart of the wizard must be from the beginning. When the user chooses to restart the wizard, any configuration the user saved previously automatically is offered for the user to accept. The user may elect to correct only a few items instead of re-entering all the data.

Since a switch may be powered on in the field without a serial connection, the switch waits 60 seconds for the user to respond to the setup wizard question in instances where no configuration files exist. If there is no response, the switch continues normal operation using the default factory configuration. While waiting for the response from the user, normal switch operation will continue, including but not limited to:

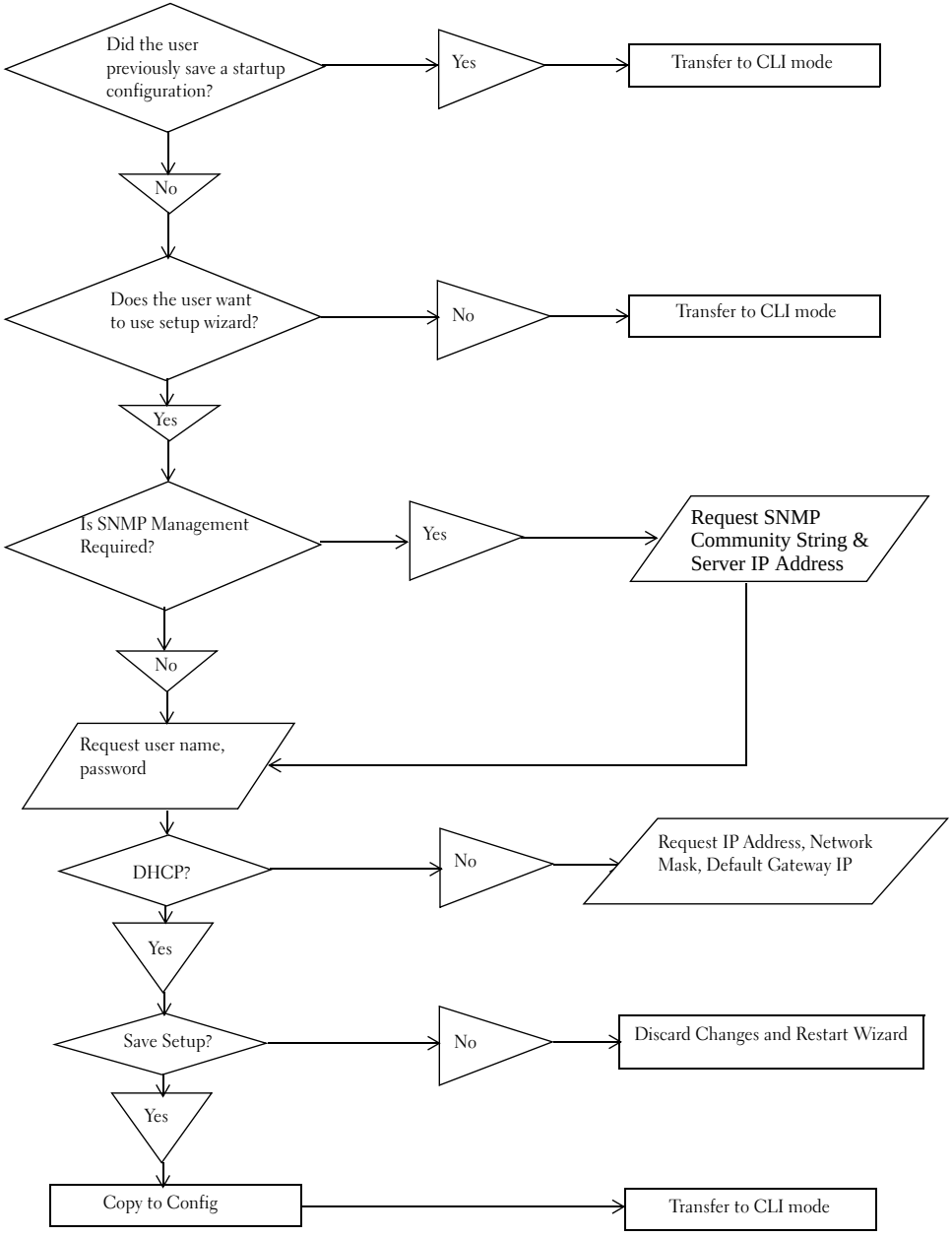
• If BOOTP/DHCP is supported and enabled by default, the switch attempts to get its address.

• The switch continues to switch traffic.

• The switch continues do MAC learning. If spanning-tree is on by default, the switch participates in the spanning-tree protocol.

Functional Flow

The functional flow diagram below illustrates the procedures for the Easy Setup Wizard.



Example Session

This section describes an Easy Setup Wizard session. Refer to the state diagram in the previous section for general flow. The following values used by the example session are not the only possible ones:

- IP address for the management VLAN is 192.168.1.100:255.255.255.0.
- The user name is *admin*, and the password should be 8-64 characters in length.
- The network management system IP address is 192.168.1.10.
- The default gateway is 192.168.1.1.
- The SNMP community string to be used is *Dell_Network_Manager.*

The setup wizard configures the initial values as defined above. After the user completes the wizard, the system is configured as follows:

- SNMPv1/2c is enabled and the community string is set up as defined above. SNMPv3 is disabled.
- The admin user account is set up as defined.
- A network management system is configured. From this management station, the user can access the SNMP, HTTP, and CLI interfaces. The user may also choose to allow all IP addresses to access these management interfaces by choosing the (0.0.0.0) IP address.
- An IP address is configured for the default management VLAN (1).
- A default gateway address is configured.

The following example contains the sequence of prompts and responses associated with running an example Dell Easy Setup Wizard session, using the input values listed above. Note in this case a static IP address for the management interface is being set up. However it may be requested that the system automatically retrieve an IP address via DHCP. If DHCP is used, the system does not request a network mask or default gateway. In this example, the user employs the setup wizard to configure the initial values as defined above.

NOTE: In the example, the possible user options are enclosed in [ ]. Also, where possible, default values are enclosed in []. If the user enters <Return> with no options defined, the default value is accepted. Help text is in parentheses.

After the switch completes the POST and is booted, the following dialog appears:

```
Welcome to Dell Easy Setup Wizard

The setup wizard guides you through the initial switch
configuration, and gets you up and running as quickly as possible.
You can skip the setup wizard, and enter CLI mode to manually
configure the switch. You must respond to the next question to run
the setup wizard within 60 seconds, otherwise the system will
continue with normal operation using the default system
configuration.
```

Would you like to run the set up wizard (you must answer this question within 60 seconds)? [Y/N) ***y***<Return>

Step 1:

The system is not configured for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager)

you can

o Setup the initial SNMP version 1 & 2 now.

o Return later and setup other SNMP accounts (for more information on setting up an SNMP version 3 account, see the user documentation).

Would you like to configure the SNMP management interface now?

[Y/N] ***y***<Return>

To configure the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell Network Manager or other management interfaces to change this setting and to add additional management systems later. For more information on adding management systems, see the user documentation.

To add a management station:

Type the SNMP community string to be used [public]:

Dell_Network_Manager<Return>

NOTE: If it is configured, the default access level is set to the highest available access for the SNMP management interface. Initially only SNMPv1/2c will be activated. SNMPv3 is disabled until you return to configure security access for SNMPv3 (e.g. engine ID, view, etc.).

Type the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station [0.0.0.0]:

192.168.1.10<Return>

Step 2:

Now we need to configure your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may set up other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the User's Guide.

To set up a user account:

Type the user name [admin]: ***admin***<Return>

Type the user password: ********<Return>

Type the user password again: ********<Return>

NOTE: If the first and second password entries are not identical, the user is prompted until they are.

NOTE: You can create additional user accounts after completing the Easy Setup Wizard. See the User's Guide for more information.

Step 3:

Next, an IP address is set up. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network using DHCP (this option requires that you have a DHCP server running on the network).

To set up an IP address:

Type the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotation marks) to automatically request an IP address from the network DHCP server. [***192.168.2.1***].

Type the IP subnet mask (A.B.C.D or /nn). [***255.255.255.0***]

Step 4:

Finally, set up the default gateway. Type the IP address of the gateway from which this network is reachable [0.0.0.0]:

This is the configuration information that has been collected:

User Account set up = admin

Password = ********

Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 0.0.0.0

```
Step 5:

If the information is correct, select (Y) to save the configuration
and copy to the start-up configuration file. If the information is
incorrect, select (N) to discard configuration and restart the
wizard: [Y/N]

Thank you for using the Dell Easy Setup Wizard. You will now enter
CLI mode.
```

Using CLI Functions and Tools

The CLI has been designed to manage the switch's configuration file system and to manage switch security. A number of resident tools exist to support these and other functions.

Configuration Management

All managed systems have software images and databases that must be configured, backed up and restored. Two software images may be stored on the system, but only one of them is active. The other one is a backup image. The same is true for configuration images, which store the configuration parameters for the switch. The system has three configuration images. One image is a memory-only image and is the current configuration image for the switch. The second image is the one that is loaded by the system when it reboots. There is one backup configuration image. The system also provides methods to back up these images to a remote system.

File System Commands

All files are stored in a flat file system. The following commands are used to perform operations on these files.

Command	Description
delete *file*	Deletes *file*.
filedescr *file description*	Adds a description to a file (up to 20 characters can be used).
copy *source destination*	Copies a file from source file to destination file.

Copying Files

The copy command not only provides a method for copying files within the file system, but also to and from remote servers. With the copy command and URLs to identify files, the user can back up images to local or remote systems or restore images from local or remote systems.

To use the **copy** command, the user specifies the source file and the destination file. For example, **copy** *tftp://remotehost/pub/backupfile backup-config* copies a file from the remote TFTP server to a local backup configuration file. In this case, if the local configuration file does not exist, then it is created by the command. If it does exist, it is overwritten. If there is not enough space on the local file system to accommodate the file, an error is flagged.

Refer to the **copy** command description in the Layer 2 commands section of the guide for command details.

Referencing External/Internal File systems

Configuration or software images are copied to or retrieved from remote file systems using TFTP and XMODEM protocols.

- **tftp:**//*server-name/path/filename* —identifies a file on a remote file system accessible through the server-name. Trivial file transfer protocol is a simplified FTP and uses a UDP port instead of TCP and does not have password protection.
- **xmodem:** *filename* —identifies the file available on the XMODEM connection.

Special System Files

The following special filenames are used to refer to special virtual system files, which are under control of the system and may not be removed or added. These file names are reserved and may not be used as user-defined files. When the user copies a local source file into one of these special files and the source file has an attached file description, it also is copied as the file description for the special file.

- **backup-config—**This file refers to the backup configuration file.
- **running-config**—This file refers to the configuration file currently active in the system. It is possible to copy the running-config image to a backup-config file or to the startup-config file.
- **startup-config**—This file refers to the special configuration image stored in flash memory which is loaded when the system next reboots. The user may copy a particular configuration file (remote or local) to this special file name and reboot the system to force it to use a particular configuration.
- **image1** & **image2** - These files refer to software images. One of these will be loaded when the system next reboots. Either image1 or image2 can be chosen for the next reboot using the command **boot system**.

CLI prevents the user from accidentally copying a configuration image onto a software image and vice versa.

Management Interface Security

This section describes the minimum set of management interface security measures implemented by the CLI. Management interface security consists of user account management, user access control and remote network/host access controls.

CLI through Telnet, SSH, Serial Interfaces

The CLI is accessible through a local serial interface, a remote telnet, or secure shell sessions. Since the serial interface requires a physical connection for access, it is used if all else fails. The serial interface is the only interface from which the user may access the Easy Setup Wizard. It is the only interface that the user can access if the remote authentication servers are down and the user has not configured the system to revert to local managed accounts.

The following rules and specifications apply to these interfaces:

- The CLI is accessible from remote telnet through the management IP address for the switch.
- The CLI is accessible from a secure shell interface.
- The CLI generates keys for SSH locally.
- The serial session defaults to 9600 baud rate, eight data bits, non-parity and one stop bit.

User Accounts Management

The CLI provides authentication for users either through remote authentication servers supporting TACACS+ or Radius or through a set of locally managed user accounts. The setup wizard asks the user to create the initial administrator account and password at the time the system is booted.

The following rules and specifications apply:

- The user may create as many a five local user accounts.
- User accounts have an access level, a user name, and a user password.
- The user is able to delete the user accounts but the user will **not** be able to delete the last level 15 account.
- The user password is saved internally in encrypted format and never appears in clear text anywhere on the CLI.
- The CLI supports TACACS+ and Radius authentication servers.
- The CLI allows the user to configure primary and secondary authentication servers. If the primary authentication server fails to respond within a configurable period, the CLI automatically tries the secondary authentication server.
- The user can specify whether the CLI should revert to using local user accounts when the remote authentication servers do not respond or if the CLI simply fails the login attempt because the authentication servers are down. This requirement applies only when the user is login through a telnet or an SSH session.
- The CLI always allows the user to log in to a local serial port even if the remote authentication server(s) are down. In this case, CLI reverts to using the locally configured accounts to allow the user to log in.

User Access Control

In addition to authenticating a user, the CLI also assigns the user access to one of two security levels. Level 1 has read-only access. This level allow the user to read information but not configure the switch. The access to this level cannot be modified. Level 15 is the special access level assigned to the superuser of the switch. This level has full access to all functions within the switch and can not be modified.

If the user account is created and maintained locally, each user is given an access level at the time of account creation. If the user is authenticated through remote authentication servers, the authentication server is configured to pass the user access level to the CLI when the user is authenticated. When Radius is used, the *Vendor-Specific Option* field returns the access level for the user. Two vendor specific options are supported. These are CISCO-AV-Pairs(Shell:priv-lvl=x) and Dell Radius VSA (user-group=x). TACACS+ provides the appropriate level of access.

The following rules and specifications apply:

- The user determines whether remote authentication servers or locally defined user authentication accounts are used.
- If authentication servers are used, the user can identify at least two remote servers (the user may choose to configure only one server) and what protocol to use with the server, TACACS+ or Radius. One of the servers is primary and the other is the secondary server (the user is not required to specify a secondary server). If the primary server fails to respond in a configurable time period, the CLI automatically attempts to authenticate the user with the secondary server.
- The user is able to specify what happens when both primary and secondary servers fail to respond. In this case, the user is able to indicate that the CLI should either use the local user accounts or reject all requests.
- Even if the user configures the CLI to fail login when the remote authentication servers are down, the CLI allows the user to log in to the serial interface authenticated by locally managed account data.

Syslogs

The CLI uses syslog support to send logging messages to a remote syslog server. The user configures the switch to generate all logging messages to a remote log server. If no remote log server exists, then the CLI maintains a rolling log of at most the last 1000 critical system events.

The following rules and specifications apply:

- The CLI permits the user to configure a remote syslog server to which all system logging messages are sent.
- Log messages are implementation-dependent but may contain debug messages, security or fault events.
- If a log server is not specified by the user, the CLI maintains at most the last 1000 critical system events. In this case, less important events are not recorded.

Security Logs

Security logs are maintained to record all security events including the following:

- User login.
- User logout.
- Denied login attempts.
- User attempt to exceed security access level.
- Denied attempts by external management system to access the system.

The security log record contains the following information:

- The user name, if available, or the protocol being accessed if the event is related to a remote management system.
- The IP address from which the user is connecting or the IP address of the remote management system.
- A description of the security event.
- A timestamp of the event

If syslog is available, the CLI sends the security log records to the syslog server. If syslog is not available, the CLI records the last 1000 security log records in a log separate from the system log records itemized above. Also in this case, the CLI suppresses repeated events from the same source and instead the CLI records one event within a period of time and includes that count as part of the log.

Management ACAL

In addition to user access control, the system also manages the access level for particular management interfaces. The system allows individual hosts or subnets to access only specific management protocols.

The user defines a management profile, which identifies management protocols such as the following:

- Telnet.
- SSH and the keying information to use for SSH.
- HTTP.
- HTTPS and the security certificate to be used.
- SNMPv1/v2c and the read and read/write community strings to be used.
- SNMPv3 and the security information for used this protocol.

For each of these management profiles, the user defines the list of hosts or subnets from which the management profiles may be used.

Other CLI Tools and Capabilities

The CLI has several other capabilities associated with its primary functions.

Terminal Paging

The terminal width and length for CLI displays is 79 characters and 25 lines, respectively. The length setting is used to control the number of lines the CLI will display before it pauses. For example, the CLI pauses at 24 lines and prompts the user with the *-more-* prompt on the 25th line. The CLI waits for the user to press either <q> or any other key. If the user presses any key except <q>, the CLI shows the next page. A <q> key stops the display and returns to the CLI prompt.

Boot Message

The boot message is a system message that is not user-configurable and is displayed when the system is booting. Displayed information includes the following:

- Operational code date
- The board type
- The CPU
- Memory size

To start the normal booting process, select item 1 in the Boot Menu. The following is a sample log for booting information.

```
Boot Menu Version: Oct 20 2004

Select an option. If no selection in 10 seconds then

operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):1


Operational Code Date: Wed Feb 8 17:02:25 2006

Uncompressing.....

50% 100%

|||||||||||||||||||||||||||||||||||||||||||||||||||

Attaching interface lo0...done

Adding 39868 symbols for standalone.

VxWorks
```

```
Copyright 1984-2002 Wind River Systems, Inc.

CPU: Motorola E500 : Unknown system version

Runtime Name: VxWorks

Runtime Version: 5.5.1

BSP version: 1.2/0

Created: Feb 8 2006, 16:40:43

WDB Comm Type: WDB_COMM_NETWORK

WDB: Ready.

Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz,
CPU:

533.33332

8 MHz

SOC unit 0 attached to PCI device BCM56304_B0

SOC unit 1 attached to PCI device BCM56304_B0

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

st_state(0) = 0x0

st_state(1) = 0x4

st_state(2) = 0x2

(Unit 1)>STACK: master on 0:2:bc:0:30:66 (1 cpu, 2 units)

STACK: attach 2 units on 1 cpu

This switch is manager of the stack.

User:
```

Boot Utility Menu

If a user is connected through the serial interface during the boot sequence, pressing the <esc> key interrupts the boot process and displays a Boot Utility Menu. Selecting item 2 displays the menu and may be typed only during the initial boot up sequence. Once the system boot up is complete, typing the escape sequence *does not* display the menu.

During the bootup sequence, if a user is connected using the serial interface, the system provides an escape key sequence to interrupt the bootup process and bring up a boot utility menu. The menu provides the users with the following:

- The boot key sequence is **2** and may be typed only during the initial bootup sequence. After the system bootup is complete, then typing the escape sequence does not have any consequence and *does not* put the user into the "boot utility menu".
- Randall supports a utility with which users can write FRU (EEPROM) data.

The following is the typical bootup sequence on the Randall switch box (with FASTPATH image):

```
Reloading all switches.


Boot code......


SDRAM 256


Boot Menu Version: Nov 10 2006
Select an option. If no selection in 10 seconds then
operational code will start.


1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2


Boot Menu Version:  24 Sep 2006


Options available
1  - Start operational code
2  - Change baud rate
3  - Retrieve event log using XMODEM
4  - Load new operational code using XMODEM
5  - Display operational code vital product data
6  - Run flash diagnostics
```

```
7  - Update boot code

8  - Delete backup image

9  - Reset the system

10 - Restore configuration to factory defaults (delete config
files)

11 - Activate Backup Image

12 - Password Recovery Procedure

[Boot Menu] 30
```

FRU Utility Menu

This is a secret option and is not displayed in the main menu. Users can bring up the secret menu using option **30**. The password for the secret menu is **pc62xxkinnick**. Option **14** under the secret menu brings up a submenu for the FRU utility. The FRU utility submenu provides options to download and set FRU, save to flash, update RU with the data saved in flash, upload FRU data, and dump FRU data. Service tag and serial number information is part of the FRU data, and users can read the service tag and serial number information from the CLI with the command **show system id**.

```
Boot Menu Version:  24 Sep 2006


Options available

1  - Start operational code

2  - Change baud rate

3  - Retrieve event log using XMODEM

4  - Load new operational code using XMODEM

5  - Display operational code vital product data

6  - Run flash diagnostics

7  - Update boot code

8  - Delete backup image

9  - Reset the system

10 - Restore configuration to factory defaults (delete config
files)

11 - Activate Backup Image

12 - Password Recovery Procedure
```

```
[Boot Menu] 30

Password: *************
Boot code utilities menu
Options are:
1  - Read/Write memory
2  - Display PCI bus
3  - Display PCI bus details
4  - Display core info and bus speeds
5  - Display file system details
6  - RAM test
7  - File system directory listing
8  - CPLD diagnostics
9  - Switch diagnostics
10 - Format file system
11 - File system test
12 - Comprehensive test (RAM, PCI, FLASH)
13 - Start vxWorks shell
14 - FRU utility menu
0  - Return to main menu
Select option (0-14): 14
FRU Utility Menu
Options are:
1 - Download data through X-Modem and store into FRU
2 - Download data through X-Modem and store into FLASH
3 - Update FRU with data stored in FLASH
4 - Upload FRU data through X-Modem
5 - Dump FRU data
0 - Return to previous menu
```

```
Select option (0-5):
```

CLI command output for the **show system id** command:

```
console>show system id


Service Tag: 89788978
Serial Number:
Asset Tag: none
 Unit     Service tag          Serial number       Asset tag
 -----    ------------         --------------      ------------
 2        89788978                                 none
```

Monitoring Traps from CLI

It is possible to connect to the CLI session and monitor the events or faults that are being sent as traps from the system. This feature is equivalent to the alarm-monitoring window in a typical network management system. The user enables events or monitor traps from the CLI by entering the command **logging console**. Traps generated by the system are dumped to all CLI sessions that have requested monitoring mode to be enabled. The **no logging console** command disables trap monitoring for the session. By default, console logging is enabled.

3

Layer 2 Commands

The chapters that follow describe commands that conform to the OSI model **data link layer (Layer 2)**. Layer 2 commands provide a logical organization for transmitting data bits on a particular medium. This layer defines the framing, addressing, and checksum functions for Ethernet packets.

4

Management ACL Commands

deny (management)

Use the **deny** command in Management Access-List Configuration mode to set conditions for the management access list.

Syntax

deny [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*] [**priority** *priority*]

deny ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*] [**priority** *priority*]

- **ethernet** *interface-number*—A valid Ethernet-routed port number.
- **vlan** *vlan-id*—A valid VLAN number.
- **port-channel** *number*—A valid routed port-channel number.
- *ip-address*—Source IP address.
- **mask** *mask*—Specifies the network mask of the source IP address.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- **service** *service*—Indicates service type. Can be one of the following: telnet, ssh, http, https or snmp.
- **priority** *priority*—Priority for the rule. (Range: 1 - 64)

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with **ethernet**, **vlan**, and **port-channel** parameters are valid only if an IP address is defined on the appropriate interface. Ensure that each rule has a unique priority.

Example

The following example shows how all ports are denied in the access-list called *mlist*.

```
console(config)# management access-list mlist

console(config-macal)# deny
```

management access-class

Use the **management access-class** command in Global Configuration mode to restrict management connections. To disable restriction, use the **no** form of this command.

Syntax

management access-class {**console-only**|*name*}

no management access-class

- *name*—A valid access-list name. (Range: 1 to 32 characters)
- **console-only**—The switch can be managed only from the console.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an access-list called *mlist* as the management access-list.

```
console(config)# management access-class mlist
```

management access-list

Use the **management access-list** command in Global Configuration mode to define an access list for management, and enter the access-list for configuration. Once in the access-list configuration mode, the denied or permitted access conditions are configured with the **deny** and **permit** commands. To remove an access list, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

- *name*—The access list name. (Range: 1 to 32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command enters the access-list configuration mode, where the denied or permitted access conditions with the **deny** and **permit** commands must be defined.

If no match criteria are defined the default is **deny**.

If reentering to an access-list context, the new rules are entered at the end of the access-list.

Use the **management access-class** command to select the active access-list.

The active management list cannot be updated or removed.

Examples

The following example shows how to configure two management interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)#management access-list mlist
console(config-macal)# permit ethernet 1/g1 priority <1-64>
console(config-macal)# permit ethernet 2/g9 priority <1-64>
console(config-macal)# exit
console(config)#management access-class mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)# management access-list mlist
console(config-macal)# deny ethernet 1/g1 priority <1-64>
console(config-macal)# deny ethernet 2/g9 priority <1-64>
console(config-macal)# permit priority <1-64>
console(config-macal)# exit
console(config) # management access-class mlist
```

permit (management)

Use the **permit** command in Management Access-List configuration mode to set conditions for the management access list.

Syntax

permit [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*] [**priority** *priority-value*]

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* |**port-channel** *number*] [**service** *service*] [**priority** *priority-value*]

- **ethernet** *interface-number*—A valid routed port number.
- **vlan** *vlan-id*—A valid VLAN number.
- **port-channel** *number*—A valid port channel number.
- *ip-address*—Source IP address.
- **mask** *mask*—Specifies the network mask of the source IP address.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- **service** *service*—Indicates service type. Can be one of the following: telnet, ssh, http, https or snmp.
- **priority** *priority-value*—Priority for the rule. (Range: 1 - 64)

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with **ethernet**, **vlan**, and **port-channel** parameters are valid only if an IP address is defined on the appropriate interface. Ensure that each rule has a unique priority.

Examples

The following example shows how to configure two management interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)#management access-list mlist
console(config-macal)# permit ethernet 1/g1 priority <1-64>
console(config-macal)# permit ethernet 2/g9 priority <1-64>
console(config-macal)# exit
console(config)# management access-class mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)# management access-list mlist
console(config-macal)# deny ethernet 1/g1 priority <1-64>
console(config-macal)# deny ethernet 2/g9 priority <1-64>
console(config-macal)# permit priority <1-64>
console(config-macal)# exit
console(config)# management access-class mlist
```

show management access-class

Use the **show management access-class** command in Privileged EXEC mode to display information about the active management access list.

Syntax

show management access-class

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the management access-list information.

```
console# show management access-class
Management access-class is enabled, using access list mlist
```

show management access-list

Use the **show management access-list** command in Privileged EXEC mode to display management access-lists.

Syntax

show management access-list [*name*]

- *name*—A valid access list name. (Range: 1 to 32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the active management access-list.

```
console# show management access-list

mlist
-----
permit priority 1 ethernet 1/g1
permit priority 2 ethernet 2/g1
! (Note: all other access implicitly denied)
```

5

User Interface Commands

enable

Use the **enable** command in User EXEC mode to enter the Privileged EXEC mode.

Syntax

enable

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to enter privileged mode.

```
console>enable
console#
```

end

Use the **end** command to get the CLI user control back to the privileged execution mode or user execution mode.

Syntax Description

end

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

No specific guidelines.

Example

```
console(config)#end

console#end

console>
```

exit (configuration)

Use the **exit** command to go to the next lower command prompt.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

Example

The following example changes the configuration mode from Interface Configuration mode to User EXEC mode.

```
console(config-if-1/g1)# exit

console(config)# exit

console#exit

console>
```

exit (EXEC)

Use the **exit** command in User EXEC mode to close an active terminal session by logging off the switch.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command mode

User Guidelines

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
console>exit
```

6

AAA Commands

aaa authentication enable

Use the **aaa authentication enable** command in Global Configuration mode to set authentication for accessing higher privilege levels. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication enable {**default**|*list-name*} *method1* [*method2...*]

no aaa authentication enable default

- **default**—Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- *list-name*—Character string used to name the list of authentication methods activated, when using access higher privilege levels. (Range: 1-12 characters)
- *method1* [*method2...*]—Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

If the **default** list is not set, only **none**, or no authentication is checked.

Command Mode

Global Configuration mode

User Guidelines

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

Create a list by entering the **aaa authentication enable** *list-name method* command where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

NOTE: Requests sent by the switch to a RADIUS or TACACS server include the username "$enabx$.", where x is the requested privilege level. For login to be authenticated on Radius and TACACS+ servers, add "$enabx$" users to them.

Example

The following example sets authentication when accessing higher privilege levels.

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

aaa authentication login

Use the **aaa authentication login** command in Global Configuration mode to set authentication at login. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication login {**default**|*list-name*} *method1* [*method2...*]

no aaa authentication login {**default**|*list-name*}

- **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name*—Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters)
- *method1* [*method2...*]—Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.

radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

If the **default** list is not set, only **none**, or no authentication is checked.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command. Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Example

The following example configures authentication login.

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

enable authentication

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

Syntax

enable authentication {**default**|*list-name*}

no enable authentication

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

Default Configuration

Uses the default set with the command **aaa authentication enable**.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

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

enable password

Use the **enable password** command in Global Configuration mode to set a local password to control access to the normal level. To remove the password requirement, use the **no** form of this command.

Syntax

enable password *password* [**encrypted**]

no enable password

- *password*—Password for this level (Range: 8- 64 characters).
- **encrypted**—Encrypted password entered, copied from another switch configuration.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines password "xxxyyyzzz" to control access to user and privilege levels.

```
console(config)# enable password xxxyyyzzz
```

ip http authentication

Use the **ip http authentication** command in Global Configuration mode to specify authentication methods for http server users. To return to the default, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2...*]

no ip http authentication

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

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

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

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Example

The following example configures the http authentication.

```
console(config)# ip http authentication radius local
```

ip https authentication

Use the **ip https authentication** command in Global Configuration mode to specify authentication methods for https server users. To return to the default configuration, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2...*]

no ip https authentication

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

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

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

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. If **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Example

The following example configures https authentication.

```
console(config)# ip https authentication radius local
```

login authentication

Use the **login authentication** command in Line Configuration mode to specify the login authentication method list for a remote telnet or console. To return to the default specified by the authentication login command, use the **no** form of this command.

Syntax

login authentication {**default**|*list-name*}

no login authentication

- **default**—Uses the default list created with the **aaa authentication login** command.
- *list-name*—Uses the indicated list created with the **aaa authentication login** command.

Default Configuration

Uses the default set with the command **aaa authentication login**.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

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

password (Line Configuration)

Use the **password** command in Line Configuration mode to specify a password on a line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

- *password*—Password for this level. (Range: 8- 64 characters)
- **encrypted**—Encrypted password to be entered, copied from another switch configuration.

Default Configuration

No password is specified.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

```
console(config-line)# password mcmxxyyy
```

password (User EXEC)

Use the **password** command in User EXEC mode to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Syntax

password

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows the prompt sequence for executing the password command.

```
console>password

Enter old password:********

Enter new password:********

Confirm new password:********
```

show authentication methods

Use the **show authentication methods** command in Privileged EXEC mode to display information about the authentication methods.

Syntax

show authentication methods

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the authentication configuration.

```
console#show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local

Enable Authentication Method Lists
----------------------------------
enableList          :  local

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   defaultList          enableList
SSH      defaultList          enableList

HTTPS       :local
HTTP        :local
DOT1X       :none
```

show users accounts

Use the **show users accounts** command in Privileged EXEC mode to display information about the local user database.

Syntax

show users accounts

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the local user database.

```
console#show users accounts
```

```
UserName            Privilege Password Password     Lockout
                              Aging    Expiry date
------------------- --------- -------- ------------ -------
admin               15        ---      ---          False
guest               1         ---      ---          False
```

show users login history

Use the **show users login history** command in Global Configuration mode to display information about the login history of users.

Syntax

show users login-history [**username** *name*]

- *name*—name of user. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example show user login history outputs.

```
console#show users login-history
Login Time            Username  Protocol  Location
--------------------  --------- --------- ---------------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:29:29  Robert    HTTP      172.16.0.8
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52   Betty    Telnet    172.16.1.7
```

username

Use the **username** command in Global Configuration mode to add a new user to the local users database. To remove a user name use the **no** form of this command.

Syntax

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

no username *name*

- *name*—The name of the user. (Range: 1-20 characters)
- *password*—The authentication password for the user. (Range: 8-64 characters)
- *level*—The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. (Range: 0-15)
- **encrypted**—Encrypted password entered, copied from another switch configuration.

Default Configuration

No user name is defined.

The default privilege level is 1.

Command Mode

Global Configuration mode

User Guidelines

This command can be used to unlock a locked user account for an already existing user.

Example

The following example configures user "bob" with password "xxxyyymmmm" and user level 15.

```
console(config)# username bob password xxxyyymmmm level 15
```

7

Address Table Commands

bridge address

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

Syntax

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

no bridge address [*mac-address*]

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

Default Configuration

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

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

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

```
console(config-if-vlan1)#bridge address 3AA2.64B3.A245 ethernet
1/g8 permanent
```

bridge aging-time

Use the **bridge aging-time** command in Global Configuration mode to set the aging time of the address. To restore the default, use the **no** form of the **bridge aging-time** command.

Syntax

bridge aging-time *seconds*

no bridge aging-time

- *seconds*—Time is the number of seconds. (Range: 10 - 1000000 seconds)

Default Configuration

300 seconds

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

In this example the bridge aging time is set to 400.

```
console(config)#bridge aging-time 400
```

bridge multicast address

Use the **bridge multicast address** command in Interface Configuration mode to register MAC-layer Multicast addresses to the bridge table and to add ports to the group statically. To deregister the MAC address, use the **no** form of the **bridge multicast address** command.

Syntax

bridge multicast address {*mac-multicast-address*|*ip-multicast-address*}

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

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

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

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If the command is executed without **add** or **remove**, the command registers only the group in the bridge database.

Static Multicast addresses can be defined only on static VLANs.

Examples

The following example registers the MAC address.

```
console(config)#interface vlan 8

console(config-if-vlan8)#bridge multicast address 0100.5e02.0203
```

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

```
console(config)#interface vlan 8

console(config-if-vlan8)#bridge multicast address 0100.5e02.0203
add ethernet 1/g1-1/g9, 1/g2
```

bridge multicast filtering

Use the **bridge multicast filtering** command in Global Configuration mode to enable filtering of Multicast addresses. To disable filtering of Multicast addresses, use the **no** form of the **bridge multicast filtering** command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Disabled. All Multicast addresses are flooded to all ports of the relevant VLAN.

Command Mode

Global Configuration mode

User Guidelines

If switches exist on the VLAN, do not change the unregistered Multicast addresses' state to drop on the switch ports.

If switches exist on the VLAN and IGMP snooping is not enabled, use the **bridge multicast forward-all** command to enable forwarding all Multicast packets to the Multicast routers.

Example

In this example, bridge Multicast filtering is enabled.

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

bridge multicast forbidden address

Use the **bridge multicast forbidden address** command in Interface Configuration mode to forbid adding a specific Multicast address to specific ports. To return to the system default, use the **no** form of this command. If routers exist on the VLAN, do not change the unregistered multicast addresses state to *drop* on the routers ports.

Syntax

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

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

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- *mac-multicast-address*—MAC Multicast address.
- *ip- multicast-address*—IP Multicast address.
- *interface-list*—Separate nonconsecutive valid Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- *port-channel-number-list*—Separate nonconsecutive valid 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, ensure that the Multicast group is registered.

Examples

In this example the MAC address 01:00:5e:02:02:03 is forbidden on port 2/g9 within VLAN 8.

```
console(config)#interface vlan 8

console(config-if-vlan8)#bridge multicast address
01:00:5e:02:02:03

console(config-if-vlan8)#bridge multicast forbidden address
01:00:5e:02:02:03 add ethernet 2/g9
```

bridge multicast forbidden forward-unregistered

Use the **bridge multicast forbidden forward-unregistered** command in Interface Configuration mode to forbid Forwarding-unregistered-multicast-addresses. Use the **no** form of this command to return to the default.

Syntax

bridge multicast forbidden forward-unregistered

no bridge multicast forbidden forward-unregistered

Default Configuration

The default for this command is *not forbidden*.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example forbids forwarding unregistered multicast addresses on VLAN8.

```
console(config-if-vlan8)#bridge multicast forbidden forward-
unregistered
```

bridge multicast forward-all

Use the **bridge multicast forward-all** command in Interface Configuration mode to enable forwarding of all Multicast packets. To restore the default, use the **no** form of the **bridge multicast forward-all** command.

Syntax

bridge multicast forward-all

no bridge multicast forward-all

Default Configuration

Forward-unregistered

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

In this example all VLAN1 Multicast packets are forwarded.

```
console(config-if-vlan1)#bridge multicast forward-all
```

bridge multicast forward-unregistered

Use the **bridge multicast forward-unregistered** command in Interface Configuration mode to enable the forwarding of unregistered multicast addresses.

Syntax

bridge multicast forward-unregistered

Default Configuration

Forward-unregistered

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If routers exist on the VLAN, do not change the unregistered multicast addresses state to *drop* on the routers ports.

NOTE: Do not use the **bridge multicast forbidden forward-unregistered** command with the **bridge multicast forward-unregistered** command on the same interface.

Example

The following example displays how to enable forwarding of unregistered multicast addresses.

```
console(config-if-vlan1)#bridge multicast forward-unregistered
```

clear bridge

Use the **clear bridge** command in Privileged EXEC mode to remove any learned entries from the forwarding database.

Syntax

clear bridge

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, the bridge tables are cleared.

```
console#clear bridge
```

port security

Use the **port security** command in Interface Configuration mode to disable the learning of new addresses on an interface. To enable new address learning, use the **no** form of the **port security** command.

Syntax

port security [**forward**|**discard**|**discard-shutdown**] [**trap** *seconds*]

no port security

- **forward**—Forwards frames with unlearned source addresses, but does not learn the address.

- **discard**—Discards frames with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown**—Discards frames with unlearned source addresses. The port is also shut down.
- **trap** *seconds*—Sends SNMP traps and defines the minimal amount of time in seconds between two consecutive traps. (Range: 1 - 1000000)

Default Configuration

Disabled - No port security

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

When port security is enabled on an interface, all dynamic entries learned up to that point are flushed, and new entries can be learned only to the limit set by the **port security max** command. The default limit is 100 dynamic MAC addresses.

Example

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

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#port security forward trap 100
```

port security max

Use the **port security max** command in Interface Configuration mode to configure the maximum addresses that can be learned on the port while the port is in port security mode. To return to the system default, use the **no** form of this command.

Syntax

port security max *max-addr*

no port security max

- *max-addr*—The maximum number of addresses that can be learning on the port. (Range: 0- 100)

Default Configuration

The default value for this command is 100.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows using this command in Ethernet Interface Configuration mode.

```
console(config-if-1/g3)# port security max 80
```

show bridge address-table

Use the **show bridge address-table** command in Privileged EXEC mode to display all entries in the bridge-forwarding database.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
console#show bridge address-table

Aging time is 300 Sec

Vlan       Mac Address           Port     Type

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

1         0000.0001.0000         1/g1    Dynamic
```

```
1        0000.8420.5010        1/g1   Dynamic
1        0000.E26D.2C2A        1/g1   Dynamic
1        0000.E89A.596E        1/g1   Dynamic
1        0001.02F1.0B33        1/g1   Dynamic
```

show bridge address-table count

Use the **show bridge address-table count** command in Privileged EXEC mode to display the number of addresses present in the Forwarding Database.

Syntax

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

- *vlan*—Specifies a valid VLAN, such as VLAN 1
- *interface*—Specifies a valid Ethernet port
- *port-channel-number*—Specifies a valid port-channel-number

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the addresses in the Forwarding Database:

```
console#show bridge address-table count

Capacity: 8192

Used: 109

Static addresses: 2

Secure addresses: 1

Dynamic addresses: 97

Internal addresses: 9
```

show bridge address-table static

Use the **show bridge address-table static** command in Privileged EXEC mode to display static entries in the bridge-forwarding database.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#show bridge address-table static

Vlan      Mac Address          Port       Type
----      --------------       -----      -----
1         0001.0001.0001       1/g1       Static
```

show bridge multicast address-table

Use the **show bridge multicast address-table** command in Privileged EXEC mode to display Multicast MAC address table information.

Syntax

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

- *vlan_id*—A valid VLAN ID value.
- *mac-multicast-address*—A valid MAC Multicast address.
- *ip- multicast-address*—A valid IP Multicast address.

- **format**—Multicast address format. Can be **ip** or **mac**.

Default Configuration

If format is unspecified, the default is **mac**.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is in the range 01:00:5e:00:00:00 through 01:00:5e:7f:ff:ff.

Example

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

```
console#show bridge multicast address-table


Vlan        MAC Address         Type                    Ports

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

1         0100.5E05.0505       Static


Forbidden ports for multicast addresses:


Vlan        MAC Address                         Ports

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

1     0100.5E05.0505
```

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

show bridge multicast filtering

Use the **show bridge multicast filtering** command in Privileged EXEC mode to display the Multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

- *vlan_id*—A valid VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#show bridge multicast filtering 1


Filtering: Disabled

VLAN: 1

Mode:

Forward-Unregistered
```

show ports security

Use the **show ports security** command in Privileged EXEC mode to display the port-lock status.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#show ports security

Port   Status    Action             Maximum  Trap     Frequency
----   ------    -----------------  -------- -------  -------
1/g1   Locked    Discard             3       Enable   100
1/g2   Unlocked  -                   28      -         -
1/g3   Locked    Discard, Shutdown   8       Disable  -
```

The following table describes the fields in this example.

Field	Description
Port	The port number.
Status	The status can be one of the following: Locked or Unlocked.
Actions	Action on violations.
Maximum	The maximum addresses that can be associated on this port in Static Learning mode or in Dynamic Learning mode.
Trap	Indicates if traps would be sent in case of violation.
Frequency	The minimum time between consecutive traps.

show ports security addresses

Use the **show ports security addresses** command in Privileged EXEC mode to display current dynamic addresses in locked ports.

Syntax

show ports security addresses {**ethernet** *interface*|**port-channel** *port-channel-number*}

- *interface*—Valid Ethernet port
- *port-channel-number*—Valid port-channel number

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays dynamic addresses for port channel number 1/g1.

```
console#show ports security addresses ethernet 1/g1


Dynamic addresses: 83


Maximum addresses: 100



Learned addresses
------- ---------
```

8

Clock Commands

show clock

Use the **show clock** command in User EXEC mode to display the time and date from the system clock.

Syntax

show clock

Default Configuration

This command has no default setting.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

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

```
console>show clock

15:29:03 Jun 17 2002

Time source is SNTP
```

show sntp configuration

Use the **show sntp configuration** command in Privileged EXEC mode to show the configuration of the Simple Network Time Protocol (SNTP).

Syntax

show sntp configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the current SNTP configuration of the device.

```
console# show sntp configuration

Polling interval: 7200 seconds

MDS Authentication keys: 8, 9

Authentication is required for synchronization

Trusted keys: 8, 9

Unicast Clients: Enabled
```

show sntp status

Use the **show sntp status** command in Privileged EXEC mode to show the status of the Simple Network Time Protocol (SNTP).

Syntax

show sntp status

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example shows the status of the SNTP.

```
console#show sntp status
```

```
Unicast servers:
server          status         Last response
---------       -----------    -------------------------
```

sntp authenticate

Use the **sntp authenticate** command in Global Configuration mode to require server authentication for received Network Time Protocol (NTP) traffic. To disable the feature, use the **no** form of this command.

Syntax

sntp authenticate

no sntp authenticate

Default Configuration

No authentication.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both Unicast and Broadcast.

Example

The following example, after defining the authentication key for SNTP, grants authentication.

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

sntp authentication-key

Use the **sntp authentication-key** command in Global Configuration mode to define an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the **no** form of this command.

Syntax

sntp authentication-key *key-number* **md5** *value*

no sntp authentication-key *number*

- *key-number*— number (Range: 1 - 4294967295)
- *value*— value (Range: 1-8 characters)

Default value

No authentication is defined.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following examples define the authentication key for SNTP.

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

sntp broadcast client enable

Use the **sntp broadcast client enable** command in Global Configuration mode to enable a Simple Network Time Protocol (SNTP) Broadcast client. To disable an SNTP Broadcast client, use the **no** form of this command.

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

This command has no user guidelines.

Example

The following example enables a Simple Network Time Protocol (SNTP) Broadcast client.

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

sntp client poll timer

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

Syntax

sntp client poll timer *seconds*

no sntp client poll timer

- *seconds* — Polling interval. (Range: 64-1024 seconds, in powers of 2)

Default Configuration

The polling interval is 64 seconds.

Command Mode

Global Configuration mode

User Guidelines

If a user enters a value which is not an exact power of two, the nearest power-of-two value is applied.

Example

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 1024 seconds.

```
console(config)# sntp client poll timer 1024
```

sntp server

Use the **sntp server** command in Global Configuration mode to configure the device to use Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. To remove a server from the list of SNTP servers, use the **no** form of this command.

Syntax

sntp server {*ip-address* | *hostname*} [**priority** *priority*] [**poll**] [**key** *key-number*]

no sntp server *ip-address*

- *ip-address* — IP address of the server.
- *hostname* — Hostname of the server. (Range: 1-158 characters)
- **poll** — Enables polling.

- *key-number* — Authentication key to use when sending packets to this peer. (Range: 1-4294967295)
- *priority*—Priority assigned to the server. (Range: 1-8)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 SNTP servers can be defined.

Use the **sntp client enable** command in Global Configuration mode to enable unicast clients globally.

Polling time is determined by the **sntp client poll timer <64-1024>** global configuration command.

Example

The following example configures the device to accept Simple Network Time Protocol (SNTP) traffic from the server at IP address 192.1.1.1.

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

sntp trusted-key

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

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

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

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

This command is relevant for both received Unicast and Broadcast.

Example

The following defines SNTP trusted-key.

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

sntp unicast client enable

Use the **sntp unicast client enable** command in Global Configuration mode to enable a client to use Simple Network Time Protocol (SNTP) predefined Unicast clients. To disable an SNTP Unicast client, use the **no** form of this command.

Syntax

sntp unicast client enable

no sntp unicast client enable

Default Configuration

The SNTP Unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp server** command to define SNTP servers.

Examples

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

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

clock timezone hours-offset

Use the **clock timezone hours-offset** [minutes *minutes-offset*] [**zone** *acronym*] command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either '0' or '\0, as appropriate.

Syntax

clock timezone hours-offset [**minutes** *minutes-offset*] [**zone** *acronym*]

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

Command Mode

Global Configuration

Default Value

No default setting

User Guidelines

No specific guidelines

Example

```
console(config)#clock timezone -5 minutes 30 zone IST
```

no clock timezone

Use the **no clock timezone** command to reset the time zone settings.

Syntax

no clock timezone

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

This command has no specific user guidelines.

Example

```
console(config)#no clock timezone
```

clock summer-time recurring

Use the **clock summer-time recurring** {**usa** | **eu** | {*week day month hh:mm week day month hh:mm*}} [**offset** *offset*] [**zone** *acronym*] command to set the summertime offset to UTC recursively every year. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

Syntax

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

- *week*—Week of the month. (Range: 1–5, first, last)
- *day*—Day of the week. (Range: The first three letters by name; sun, for example.)
- *month*—Month. (Range: The first three letters by name; jan, for example.)
- *hh:mm*—Time in 24-hour format in hours and minutes. (Range: hh: 0–23, mm: 0–59)
- *offset*—Number of minutes to add during the summertime. (Range:1–1440)
- *acronym*—The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

Default Value

No default setting

Command Mode

Global Configuration

User Guidelines

No specific guidelines

Examples

```
console(config)# clock summer-time recurring 1 sun jan 00:10 2 mon
mar 10:00 offset 1 zone ABC
```

clock summer-time date

Use the **clock summer-time date** {**date**|**month**} {**month**|**date**} *year hh:mm* {**date**|**month**} {**month**|**date**} *year hh:mm* [**offset** *offset*] [**zone** *acronym*] command to set the summertime offset to UTC. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

Syntax

clock summer-time date {**date**|**month**} {**month**|**date**} *year hh:mm* {**date**|**month**} {**month**|**date**} *year hh:mm* [**offset** *offset*] [**zone** *acronym*]

- *date*—Day of the month. (Range: 1–31)
- *month*—Month. (Range: The first three letters by name; jan, for example.)
- *year*—Year. (Range: 2000–2097)
- *hh:mm*—Time in 24-hour format in hours and minutes. (Range: hh: 0–23, mm: 0–59)
- *offset*—Number of minutes to add during the summertime. (Range: 1–1440)
- *acronym*—The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines

Examples

```
console(config)# clock summer-time date 1 Apr 2007 02:00 28 Oct
2007 offset 90 zone EST
```

or

```
console(config)# clock summer-time date Apr 1 2007 02:00 Oct 28
2007 offset 90 zone EST
```

no clock summer-time recurring

Use the **no clock summer-time recurring** command to reset the recurring summertime configuration.

Syntax Description

no clock summer-time recurring

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines

Example

```
console(config)#no clock summer-time recurring
```

show clock

Use the **show clock** command to display the time and date from the system clock. Use the **show clock detail** command to show the time zone and summertime configuration.

Syntax Description

show clock [**detail**]

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines

Example

The following example shows the time and date only.

```
console# show clock

15:29:03 PDT(UTC-7) Jun 17 2005

Time source is SNTP
```

The following example shows the time, date, timezone, and summertime configuration.

```
console# show clock detail

15:29:03 PDT(UTC-7) Jun 17 2005

Time source is SNTP

Time zone:

Acronym is PST

Offset is UTC-7

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.
```

9

Denial of Service Commands

dos-control firstfrag

Use the **dos-control firstfrag** command in Global Configuration mode to enable Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller than the configured value, the packets are dropped.

Syntax

dos-control firstfrag [*size*]

no dos-control firstfrag

- *size* —TCP header size. (Range: 0-255). The default TCP header size is 20. ICMP packet size is 512.

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a minimum TCP header size of 20. Packets entering with a smaller header size are dropped.

```
console(config)#dos-control firstfrag 20
```

dos-control icmp

Use the **dos-control icmp** command in Global Configuration mode to enable Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets are dropped.

Syntax

dos-control icmp [*size*]

no dos-control icmp

- *size* — Maximum ICMP packet size. (Range: 0-1023). If size is unspecified, the value is 512.

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates the Maximum ICMP Packet Denial of Service protection with a maximum packet size of 1023.

```
console(config)#dos-control icmp 1023
```

dos-control l4port

Use the **dos-control l4port** command in Global Configuration mode to enable L4 Port Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets are dropped.

Syntax

dos-control l4port

no dos-control l4port

Default Configuration

Denial of Service is disabled.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example activates L4 Port Denial of Service protection.

```
console(config)#dos-control l4port
```

dos-control sipdip

Use the **dos-control sipdip** command in Global Configuration mode to enable Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets is dropped if the mode is enabled.

Syntax
dos-control sipdip

no dos-control sipdip

Default Configuration
Denial of Service is disabled.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example activates SIP=DIP Denial of Service protection.

```
console(config)#dos-control sipdip
```

dos-control tcpflag

Use the **dos-control tcpflag** command in Global Configuration mode to enable TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024, having TCP

Control Flags set to 0 and TCP Sequence Number set to 0, having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0, or having TCP Flags SYN and FIN both set, the packets are dropped.

Syntax

dos-control tcpflag

no dos-control tcpflag

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example activates TCP Flag Denial of Service protections.

```
console(config)#dos-control tcpflag
```

dos-control tcpfrag

Use the **dos-control tcpfrag** command in Global Configuration mode to enable TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets are dropped.

Syntax

dos-control tcpfrag

no dos-control tcpfrag

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates TCP Fragment Denial of Service protection.

```
console(config)#dos-control tcpfrag
```

show dos-control

Use the **show dos-control** command in Privileged EXEC mode to display Denial of Service configuration information.

Syntax

show dos-control

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays Denial of Service configuration information.

```
console#show dos-control

SIPDIP Mode..................................... Disable

First Fragment Mode.......................... Disable

Min TCP Hdr Size............................. 20

TCP Fragment Mode........................... Disable

TCP Flag Mode................................ Disable

L4 Port Mode..................................... Disable

ICMP Mode....................................... Disable

Max ICMP Pkt Size........................... 512
```

10

DHCP Filtering Commands

ip dhcp filtering

Use the **ip dhcp filtering** command in Global Configuration mode to enable DHCP filtering globally. To disable DHCP filtering globally, use the **no** form of this command.

Syntax

ip dhcp filtering

no ip dhcp filtering

Default Configuration

DHCP Filtering is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable DHCP filtering globally.

```
console(config)#ip dhcp filtering
```

ip dhcp filtering trust

Use the **ip dhcp filtering trust** command in Interface Configuration mode to configure an interface as trusted. Any DHCP response received on a trusted port will be forwarded. To configure an interface as untrusted, use the **no** form of this command.

Syntax

ip dhcp filtering trust

no ip dhcp filtering trust

Default Configuration

Any DHCP response received on a trusted port will be forwarded.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to configure an interface as trusted for DHCP snooping purposes.

```
console(config-if-1/g3)#ip dhcp filtering trust
```

show ip dhcp filtering

Use the **show ip dhcp filtering** command in Privileged EXEC mode to display the DHCP snooping configuration.

Syntax

show ip dhcp filtering

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DHCP filtering configuration.

```
console#show ip dhcp filtering

Switch DHCP filtering is enabled

Interface                Trusted
-------------------      -------
1/g1                     no
```

```
1/g6                          yes
```

11

Ethernet Configuration Commands

clear counters

Use the **clear counters** command in Privileged EXEC mode to clear statistics on an interface.

Syntax

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

- *interface*—Valid Ethernet port. The full syntax is: *unit/port*
- *port-channel-number*—Valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In the following example, the counters for port 1/g1 are cleared.

```
console#clear counters ethernet 1/g1
```

description

Use the **description** command in Interface Configuration mode to add a description to an interface. To remove the description use the **no** form of this command.

Syntax

description *string*

no description

- *string*—Comment or a description of the port attached to this interface. (Range: 1 to 64 characters)

Default Configuration

By default, the interface does not have a description.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example adds a description to the Ethernet port 5.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)# description RD_SW#3
```

duplex

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

Syntax

duplex {**half** | **full**}

no duplex

- **half**—Force half-duplex operation
- **full**—Force full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Ports that are set for 1000 Mbps operation can not be set for half duplex operation.

Example

The following example configures the duplex operation of Ethernet port 5 to force full duplex operation.

```
console(config)# interface ethernet 1/g5

console(config-if-1/g5)# duplex full
```

flowcontrol

Use the **flowcontrol** command in Global Configuration mode to configure the flow control. To disable flow control, use the **no** form of this command.

Syntax

flowcontrol

no flowcontrol

Default Configuration

Flow Control is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

In the following example, flow control is enabled.

```
console(config)# flowcontrol
```

interface ethernet

Use the **interface ethernet** command in Global Configuration mode to enter the interface configuration mode to configure an Ethernet type interface.

Syntax

interface ethernet *interface*

- *interface*—Valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables port 5/g18 for configuration.

```
console(config)# interface ethernet 5/g18
```

interface range ethernet

Use the **interface range ethernet** command in Global Configuration mode to execute a command on multiple ports at the same time.

Syntax

interface range ethernet {*port-range* | **all**}

- *port-range*—List of valid ports to configure. Separate non consecutive ports with a comma and no spaces; use a hyphen to designate a range of ports. For more detailed information, refer to the Operating on Multiple Objects (Range) discussion in the Using the CLI chapter.
- **all**—All Ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

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

Example

The following example shows how ports 5/g18 to 5/g20 and ports 3/g1 to g24 are grouped to receive the same command.

```
console(config)# interface range ethernet 5/g18-5/g20,3/g1-3/g24
console(config-if)#
```

mdix

Use the **mdix** command in Interface Configuration mode to enable cable crossover on a given interface. To disable crossover, use the **no** form of this command.

Syntax

mdix {on | auto}

no mdix

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

Default Configuration

Automatic crossover is enabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

In the following example, automatic crossover is enabled on gigabit Ethernet port 5 of unit 1.

```
console(config)# interface ethernet 1/g5

console(config-if-1/g5)# mdix auto
```

mtu

Use the **mtu** command in Interface Configuration mode to enable jumbo frames on an interface by adjusting the maximum size of a packet. To return to the default setting, use the **no** form of this command.

Syntax

mtu *bytes*

no mtu

- *bytes* —Number of bytes (Range: 1518-9216)

Default Configuration

The default number of bytes is 1518 (1522 bytes of VLAN-tagged frames).

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The value set allows an additional four bytes for the VLAN tag.

Example

The following example of the mtu command increases maximum packet size to 9216 bytes.

```
console(config-if-1/g5)#mtu 9216
```

negotiation

Use the **negotiation** command in Interface Configuration mode to enable auto-negotiation operation for the speed and duplex parameters of a given interface. To disable negotiation, use the **no** form of this command.

Syntax

negotiation [**capability1** [**capability2**...**capability5**]]

no negotiation

- **capabilities**—Specifies capabilities to advertise. (Possible values: 10h, 10f, 100h, 100f and 1000f)

Default Configuration

If unspecified, defaults to list of all capabilities of the port.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Entering the command negotiation with no parameters enables all capabilities. Note that if you have previously entered negotiation with capabilities, this action overwrites the previous configuration so that all capabilities are enabled.

Example

The following example enables auto negotiations on gigabit Ethernet port 5 of unit 1.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#negotiation
```

show interfaces advertise

Use the **show interfaces advertise** command in Privileged EXEC mode to display information about auto-negotiation advertisement.

Syntax

show interfaces advertise [**ethernet** *interface*]

- *interface*—A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display information about auto negotiation advertisement.

```
console#show interfaces advertise
Port  Type        Neg      Operational Link Advertisement
----  ----        ---      ------------------------------
1/g2  1G-Copper   Enable   1000f, 100f, 100h, 10f, 10h
1/g2  1G-Copper   Enable   1000f


console# show interfaces advertise ethernet 1/g1
Port: Ethernet 1/g1
Type: 1G-Copper
Link state: Up
Auto negotiation: enabled
10h 10f 100h 100f 1000f
Admin Local Link ------ ------ ------ ------ ------
    Advertisement yes     yes    yes    yes     no
```

show interfaces configuration

Use the **show interfaces configuration** command in User EXEC mode to display the configuration for all configured interfaces.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Modes

User EXEC mode

User Guidelines

This command has no use guidelines.

Example

The following example displays the configuration for all configured interfaces:

```
console>show interfaces configuration


Port   Type               Duplex  Speed    Neg   MDIX  Admin
                                                Mode  State
-----  -----------------  ------  -------  ----  ----  -----
1/g1   Gigabit - Level    Full    100      Auto  Auto   Up
1/g2   Gigabit - Level    Full    100      Auto  Auto   Up
1/g3   Gigabit - Level    Full    100      Auto  Auto   Up
```

The displayed port configuration information includes the following:

Field	Description
Port	The port number.
Port Type	The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
Duplex	Displays the port Duplex status.
Speed	Refers to the port speed.
Neg	Describes the Auto-negotiation status.
MDIX Mode	Displays the Auto-crossover status.
Admin State	Displays whether the port is enabled or disabled.

show interfaces counters

Use the **show interfaces counters** command in User EXEC mode to display traffic seen by the interface.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Modes

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays traffic seen by the physical interface:

```
console>show interfaces counters

Port   InOctets    InUcastPkts

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

1/g1   183892      1289
```

```
3/g1  123899      1788

Port  OutOctets   OutUcastPkts
----  ----------  ---------
1/g1  9188        9
2/g1  0           0
3/g1  8789        27


Ch    InOctets    InUcastPkts
----  ----------  ---------
1     27889       928

Ch    OutOctets   OutUcastPkts
----  ----------  ---------
1     23739       882
```

The following example displays counters for Ethernet port 1/g1.

```
console#show interfaces counters ethernet 1/g1
Port  InOctets    InUcastPkts
----  ----------  ---------
1/g1  183892      1289

Port  OutOctets    OutUcastPkts
----  ----------   ---------
1/g1  9188         9

Alignment Errors: 17
FCS Errors: 8
Single Collision Frames: 0
Multiple Collision Frames: 0
```

```
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display:

Field	Description
InOctets	Counted received octets.
InUcastPkts	Counted received Unicast packets.
InMcastPkts	Counted received Multicast packets.
InBcastPkts	Counted received Broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted Unicast packets.
OutMcastPkts	Counted transmitted Multicast packets.
OutBcastPkts	Counted transmitted Broadcast packets.
Alignment Errors	A count of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	Counted frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	A count of frames that are involved in a multiple collision, and are subsequently transmitted successfully
Deferred Transmissions	A count of frames for which the first transmission attempt is delayed because the medium is busy
Late Collisions	Counted times that a collision is detected later than one slot time into the transmission of a packet.
Excessive Collisions	Counted frames for which transmission fails due to excessive collisions.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	A count of frames for which reception fails due to an internal MAC sublayer receive error.

Field	Description
Received Pause Frames	A count of MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

show interfaces description

Use the **show interfaces description** command in User EXEC mode to display the description for all configured interfaces.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Modes

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the description for the interface 1/g1.

```
console>show interfaces description

Port Description

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

1/g1 Port that should be used for management only

2/g1

2/g2
```

```
Ch     Description
----   -----------
1      Output
```

show interfaces status

Use the **show interfaces status** command in User EXEC mode to display the status for all configured interfaces.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the status for all configured interfaces.

```
console>show interfaces status
Port   Type         Duplex  Speed  Neg   MDIX  Link
                                          Mode  State
----   ----------   ------  -----  ----  ----  -----
1/g1   1G-Combo-c   Full    100    Auto  on    Up
2/g1   100-Copper   Full    100    Off   off   Down*
2/g2   1G-Fiber     Full    1000   Off   on    Up


Ch     Type  Duplex  Speed  Neg   Link
```

```
                                        State
----   ----   ------   -----   ----   -----
1      1000   Full     1000    Off    Up

*: The interface was suspended by the system.
```

The displayed port status information includes the following:

Field	Description
Port	The port number.
Type	The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
Duplex	Displays the port Duplex status.
Speed	Refers to the port speed.
Neg	Describes the Auto-negotiation status.
MDIX Mode	Displays the Auto-crossover status.
Link State	Displays the Link Aggregation status.

show statistics ethernet

Use the **show statistics ethernet** command in Privileged EXEC mode to display detailed statistics for a specific port or for the entire switch.

Syntax

show statistics ethernet { <*unit*>/<*port-type*><*port*> | **switchport** }

- <*unit*>/<*port-type*><*port*>—Displays statistics for a valid unit/port:
  <*unit*>—Physical switch identifier within the stack. Values are *1-12*.
  <*port-type*>— Values are **g** for gigabit Ethernet port, or **xg** for 10 gigabit Ethernet port.
  <*port*>—port number. Values are *1-24* or *1-48* in the case of port_type g, and 1-4 for port_type xg.
  Example: xg2 is the 10 gigabit Ethernet port 2.
- **switchport**—Displays statistics for the entire switch.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Examples

The following examples show statistics for port 1/g1 and for the entire switch.

```
console#show statistics ethernet 1/g1
Total Packets Received (Octets)..... 779533115
Packets Received 64 Octets..... 48950
Packets Received 65-127 Octets..... 482426
Packets Received 128-255 Octets..... 101084
Packets Received 256-511 Octets..... 163671
Packets Received 512-1023 Octets..... 4824
Packets Received 1024-1518 Octets..... 479543
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 94516
Packets RX and TX 65-127 Octets..... 483312
Packets RX and TX 128-255 Octets..... 101329
Packets RX and TX 256-511 Octets..... 163696
Packets RX and TX 512-1023 Octets..... 4982
Packets RX and TX 1024-1518 Octets..... 479845
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0
Total Packets Received Without Errors..... 1280498
Unicast Packets Received..... 1155457
Multicast Packets Received..... 48339
```

```
--More-- or (q)uit
Broadcast Packets Received..................... 76702
Total Packets Received with MAC Errors......... 0
Jabbers Received............................... 0
Fragments/Undersize Received................... 0
Alignment Errors............................... 0
FCS Errors..................................... 0
Overruns....................................... 0
Total Received Packets Not Forwarded........... 91
Local Traffic Frames........................... 0
802.3x Pause Frames Received................... 0
Unacceptable Frame Type........................ 91
Multicast Tree Viable Discards................. 0
Reserved Address Discards...................... 0
Broadcast Storm Recovery....................... 0
CFI Discards................................... 0
Upstream Threshold............................. 0
Total Packets Transmitted (Octets)............. 3604988
Packets Transmitted 64 Octets.................. 45566
Packets Transmitted 65-127 Octets.............. 886
Packets Transmitted 128-255 Octets............. 245
--More-- or (q)uit
Packets Transmitted 256-511 Octets............. 25
Packets Transmitted 512-1023 Octets............ 158
Packets Transmitted 1024-1518 Octets........... 302
Max Frame Size................................. 1518
Total Packets Transmitted Successfully......... 47182
Unicast Packets Transmitted.................... 2746
Multicast Packets Transmitted.................. 44432
```

```
Broadcast Packets Transmitted..................... 4
Total Transmit Errors............................. 0
FCS Errors........................................ 0
Tx Oversized...................................... 0
Underrun Errors................................... 0
Total Transmit Packets Discarded.................. 0
Single Collision Frames........................... 0
Multiple Collision Frames......................... 0
Excessive Collision Frames........................ 0
Port Membership Discards.......................... 0
802.3x Pause Frames Transmitted................... 0
GVRP PDUs received................................ 0
--More-- or (q)uit
GVRP PDUs Transmitted............................. 0
GVRP Failed Registrations......................... 0
BPDU: sent 44432, received 0
EAPOL Frames Transmitted.......................... 0
EAPOL Start Frames Received....................... 0
Time Since Counters Last Cleared.................. 1 day 0 hr 41 min
44 sec

console#show statistics ethernet switchport

Total Packets Received (Octets)................... 16877295
Unicast Packets Received.......................... 1608
Multicast Packets Received........................ 48339
Broadcast Packets Received........................ 69535
Receive Packets Discarded......................... 0
Octets Transmitted................................ 6451988
```

```
Packets Transmitted Without Errors..... 91652
Unicast Packets Transmitted..... 2746
Multicast Packets Transmitted..... 88892
Broadcast Packets Transmitted..... 14
Transmit Packets Discarded..... 0
--More-- or (q)uit
Most Address Entries Ever Used..... 141
Address Entries Currently in Use..... 124
Maximum VLAN Entries..... 1024
Most VLAN Entries Ever Used..... 6
Static VLAN Entries..... 6
Dynamic VLAN Entries..... 0
VLAN Deletes..... 0
Time Since Counters Last Cleared..... 1 day 0 hr 42 min
13 sec
console#
```

show storm-control

Use the **show storm-control** command in Privileged EXEC mode to display the configuration of storm control.

Syntax

show storm-control [**all** |*interface*]

- *interface*—Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example shows storm control configurations for all valid Ethernet ports. The second example shows flow control mode status.

```
console#show storm-control all

       Bcast   Bcast   Mcast   Mcast   Ucast   Ucast
Intf   Mode    Level   Mode    Level   Mode    Level
------ ------- ------- ------- ------- ------- -------
1/g1   Disable 5       Disable 5       Disable 5
1/g2   Disable 5       Disable 5       Disable 5
1/g3   Disable 5       Disable 5       Disable 5
1/g4   Disable 5       Disable 5       Disable 5

console#show storm-control

802.3x Flow Control Mode..................... Disable
```

shutdown

Use the **shutdown** command in Interface Configuration mode to disable an interface. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Examples

The following example disables Ethernet port 1/g5.

```
console(config)#interface ethernet 1/g5

console(config-if-1/g5)# shutdown
```

The following example re-enables ethernet port 1/g5.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)# no shutdown
```

speed

Use the **speed** command in Interface Configuration mode to configure the speed of a given Ethernet interface when not using auto-negotiation. To restore the default, use the **no** form of this command.

Syntax

speed [10 | 100 | 1000]

no speed

- 10—Configures the port to 10 Mbps operation.
- 100—Configures the port to 100 Mbps operation.
- 1000—Configures the port to 1000 Mbps operation.

Default Configuration

This command has no default setting.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the speed operation of Ethernet port 1/g5 to force 100-Mbps operation.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#speed 100
```

storm-control broadcast

Use the **storm-control broadcast** command in Interface Configuration mode to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Syntax

storm-control broadcast [**level** *rate*]

no storm-control broadcast

- *rate*—Percentage of port bandwidth to allow. (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

console(config-if-1/g1)#storm-control broadcast level 5

storm-control multicast

Use the **storm-control multicast** command in Interface Configuration mode to enable multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Syntax

storm-control multicast [**level** *rate*]

no storm-control multicast

- *rate*—Maximum packets per second of multicast traffic on a port. (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

console(config-if-1/g1)#storm-control multicast level 5

storm-control unicast

Use the **storm-control unicast** command in Interface Configuration mode to enable unknown unicast storm control for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Syntax

storm-control unicast [**level** *rate*]

no storm-control unicast

- *rate*—Maximum packets per second of unicast traffic on a port. (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

console(config-if-1/g1)#storm-control unicast level 5

12

GVRP Commands

clear gvrp statistics

Use the **clear gvrp statistics** command in Privileged EXEC mode to clear all the GVRP statistics information.

Syntax

clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears all the GVRP statistics information on port 1/g8.

```
console# clear gvrp statistics ethernet 1/g8
```

garp timer

Use the **garp timer** command in Interface Configuration mode to adjust the GARP application join, leave, and leaveall GARP timer values. To reset the timer to default values, use the **no** form of this command.

Syntax

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

no garp timer

- **join**—Indicates the time in centiseconds that PDUs are transmitted.
- **leave**—Indicates the time in centiseconds that the device waits before leaving its GARP state.
- **leaveall**—Used to confirm the port within the VLAN. The time is the interval between messages sent, measured in centiseconds.
- *timer_value*—Timer values in centiseconds. The range is 10-100 for **join**, 30-600 for **leave**, and 200-6000 for **leaveall**.

Default Configuration

The default timer values are as follows:

- Join timer—20 centiseconds
- Leave timer—60 centiseconds
- Leaveall timer—1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

The following *relationships* for the various timer values must be maintained:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, the GARP application will not operate successfully.

The *timer_value* setting must be a multiple of 10.

Example

The following example sets the leave timer for port 1/g8 to 90 centiseconds.

```
console (config)# interface ethernet 1/g8
console (config-if-1/g8)# garp timer leave 90
```

gvrp enable (global)

Use the **gvrp enable (global)** command in Global Configuration mode to enable GVRP globally on the switch. To disable GVRP globally on the switch, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables GVRP on the device.

```
console(config)#gvrp enable
```

gvrp enable (interface)

Use the **gvrp enable** command in Interface Configuration mode to enable GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces by default.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

An Access port cannot join dynamically to a VLAN because it is always a member of only one VLAN.

Membership in untagged VLAN would be propagated in a same way as a tagged VLAN. In such cases it is the administrator's responsibility to set the PVID to be the untagged VLAN VID.

Example

The following example enables GVRP on ethernet 1/g8.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#gvrp enable
```

gvrp registration-forbid

Use the **gvrp registration-forbid** command in Interface Configuration mode to deregister all VLANs on a port and prevent any dynamic registration on the port. To allow dynamic registering for VLANs on a port, use the **no** form of this command.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registering and deregistering for each VLAN on the port is not forbidden.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port 1/g8.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#gvrp registration-forbid
```

gvrp vlan-creation-forbid

Use the **gvrp vlan-creation-forbid** command in Interface Configuration mode to disable dynamic VLAN creation. To disable dynamic VLAN creation, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration

By default, dynamic VLAN creation is enabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example disables dynamic VLAN creation on port 1/g8.

```
console(config)#interface ethernet 1/g8

console(config-if-1/g8)#gvrp vlan-creation-forbid
```

show gvrp configuration

Use the **show gvrp configuration** command in Privileged EXEC mode to display GVRP configuration information. Timer values are displayed. Other data shows whether GVRP is enabled and which ports are running GVRP.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display GVRP configuration information:

```
console# show gvrp configuration
                Join          Leave        LeaveAll       Port
 Interface      Timer         Timer         Timer       GVRP Mode
              (centisecs)   (centisecs)   (centisecs)
-----------  -----------   -----------   -----------   -----------
1/g1         20            60            1000          Disabled
1/g2         20            60            1000          Disabled
1/g3         20            60            1000          Disabled
1/g4         20            60            1000          Disabled
1/g5         20            60            1000          Disabled
1/g6         20            60            1000          Disabled
1/g7         20            60            1000          Disabled
1/g8         20            60            1000          Disabled
1/g9         20            60            1000          Disabled
1/g10        20            60            1000          Disabled
1/g11        20            60            1000          Disabled
1/g12        20            60            1000          Disabled
1/g13        20            60            1000          Disabled
1/g14        20            60            1000          Disabled
1/g15        20            60            1000          Disabled
1/g16        20            60            1000          Disabled
1/g17        20            60            1000          Disabled
1/g18        20            60            1000          Disabled
```

show gvrp error-statistics

Use the **show gvrp error-statistics** command in User EXEC mode to display GVRP error statistics.

Syntax

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

- *interface*—A valid Ethernet interface.

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

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays GVRP error statistics information.

```
console>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
----  -------    -------     -------    -------    --------
1/g1     0          0           0          0          0
1/g2     0          0           0          0          0
1/g3     0          0           0          0          0
1/g4     0          0           0          0          0
```

show gvrp statistics

Use the **show gvrp statistics** command in User EXEC mode to display GVRP statistics.

Syntax

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

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

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

This example shows output of the **show gvrp statistics** command.

```
console>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                  JIn : Join In Sent
sEmp : Empty Sent                       sLIn : Leave In Sent
sLE  : Leave Empty Sent                 sLA  : Leave All Sent

Port   rJE  rJIn  rEmp  rLIn  rLE   rLA  sJE  sJIn  sEmp  sLIn  sLE  sLA
----   ---  ----  ----  ----  ---   ---  ---  ---   ---   ----  ---- ---
1/g1    0    0     0      0     0     0    0    0     0     0      0    0
1/g2    0    0     0      0     0     0    0    0     0     0      0    0
1/g3    0    0     0      0     0     0    0    0     0     0      0    0
1/g4    0    0     0      0     0     0    0    0     0     0      0    0
```

```
1/g5    0    0    0    0    0    0    0    0    0    0    0    0
1/g6    0    0    0    0    0    0    0    0    0    0    0    0
1/g7    0    0    0    0    0    0    0    0    0    0    0    0
1/g8    0    0    0    0    0    0    0    0    0    0    0    0
```

13

IGMP Snooping Commands

ip igmp snooping (global)

Use the **ip igmp snooping** command in Global Configuration mode to globally enable Internet Group Management Protocol (IGMP) snooping.

Syntax

ip igmp snooping [*vlan-id*]

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping is enabled on static VLANs only and is not enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping.

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

ip igmp snooping (interface)

Use the **ip igmp snooping** command in Interface Configuration mode to enable Internet Group Management Protocol (IGMP) snooping on a specific interface. To disable IGMP snooping on an Ethernet interface, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

IGMP snooping can be enabled on Ethernet interfaces.

Example

The following example enables IGMP snooping.

```
console(config-if-1/g1)#ip igmp snooping
```

ip igmp snooping host-time-out

Use the **ip igmp snooping host-time-out** command in Interface Configuration mode to configure the host-time-out. If an IGMP report for a Multicast group is not received for a host time-out period from a specific port, this port is deleted from the member list of that Multicast group. To reset to the default host time-out, use the **no** form of this command.

Syntax

ip igmp snooping host-time-out *time-out*

no ip igmp snooping host-time-out

- *time-out*—Host timeout in seconds. (Range: 1 - 2147483647)

Default Configuration

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The timeout should be more than sum of response time and twice the query interval.

Example

The following example configures the host timeout to 300 seconds.

```
console(config-if-1/g1)#ip igmp snooping host-time-out 300
```

ip igmp snooping leave-time-out

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

Syntax

ip igmp snooping leave-time-out [*time-out* | **immediate-leave**]

no ip igmp snooping leave-time-out

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

Default Configuration

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

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP Query.

Use **immediate leave** only where there is only one host connected to a port.

Example

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

```
console(config-if-1/g1)#ip igmp snooping leave-time-out 60
```

ip igmp snooping mrouter-time-out

Use the **ip igmp snooping mrouter-time-out** command in Interface Configuration mode to configure the mrouter-time-out. This command is used for setting the aging-out time after Multicast router ports are automatically learned. To reset to the default mrouter-time-out, use the **no** form of this command.

Syntax

ip igmp snooping mrouter-time-out *time-out*

no ip igmp snooping mrouter-time-out

- *time-out*—mrouter timeout in seconds for IGMP. (Range: 1 - 2147483647)

Default Configuration

The default value is 300 seconds.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the mrouter timeout to 200 seconds.

```
console(config-if-1/g1)#ip igmp snooping mrouter-time-out 200
```

show ip igmp snooping groups

Use the **show ip igmp snooping groups** command in User EXEC mode to display the Multicast groups learned by IGMP snooping.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]

- *vlan_id*—Specifies a VLAN ID value.
- *ip-multicast-address*—Specifies an IP Multicast address.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

To see the full Multicast address table (including static addresses) use the **show bridge address-table** command.

Example

The example shows Multicast groups learned by IGMP snooping for all VLANs.

```
console>show ip igmp snooping groups

Vlan    IP Address                  Ports

----    -----------               -------
```

```
1      224-239.130|2.2.3          1/g1, 2/g2
19     224-239.130|2.2.8          1/g9-g11


IGMP Reporters that are forbidden statically:
---------------------------------------------
Vlan   IP Address                Ports
----   ------------------   -------------------
1      224-239.130|2.2.3         1/g19
```

show ip igmp snooping interface

Use the **show ip igmp snooping interface** command in Privileged EXEC mode to display the IGMP snooping configuration.

Syntax

show ip igmp snooping interface *interface* {ethernet *interface* | port-channel *port-channel-number*}

- *interface*—Valid Ethernet port. The full syntax is *unit/port*.
- *port-channel-number*—Valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The example displays IGMP snooping information.

```
console#show ip igmp snooping interface 1/g1
Slot/Port..................................... 1/g1
IGMP Snooping Admin Mode...................... Disabled
Fast Leave Mode............................... Disabled
Group Membership Interval..................... 260
```

```
Max Response Time..............................  10

Multicast Router Present Expiration Time.......  300
```

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** command in Privileged EXEC mode to display information on dynamically learned Multicast router interfaces.

Syntax

show ip igmp snooping mrouter

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows IGMP snooping mrouter information.

```
console#show igmp snooping mrouter

Port.....................................1/g1
```

ip igmp snooping (VLAN)

Use the **ip igmp snooping** command in VLAN Configuration mode to enable IGMP snooping on a particular interface or on all interfaces participating in a VLAN. To disable IGMP snooping use the **no** form of this command.

Syntax

ip igmp snooping *vlan-id*

no ip igmp snooping

Default Configuration

IGMP snooping is disabled on VLAN interfaces by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping on VLAN 2.

```
console(config-vlan)#ip igmp snooping 2
```

ip igmp snooping fast-leave

This command enables or disables IGMP Snooping fast-leave mode on a selected VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. The **no** form of this command disables IGMP Snooping fast-leave mode on a VLAN.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This setting prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Syntax

ip igmp snooping fast-leave *vlan-id*

no ip igmp snooping fast-leave

- *vlan id*—Number assigned to the VLAN.

Default Configuration

IGMP snooping fast-leave mode is disabled on VLANs by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping fast-leave mode on VLAN 2.

```
console(config-vlan)#ip igmp snooping fast-leave 2
```

ip igmp snooping groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds. The **no** form of this command sets the IGMPv3 Group Membership Interval time to the default value.

Syntax

ip igmp snooping groupmembership-interval *vlan-id seconds*

no ip igmp snooping groupmembership-interval

- *vlan-id* —Number assigned to the VLAN
- seconds—IGMP group membership interval time in seconds. (Range: 1-2147483647)

Default Configuration

The default group membership interval time is 260 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an IGMP snooping group membership interval of 520 seconds.

```
console(config-vlan)#ip igmp snooping groupmembership-interval 2
520
```

ip igmp snooping maxresponse

This command sets the IGMP Maximum Response time on a particular VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds. The **no** form of this command sets the maximum response time on the VLAN to the default value.

Syntax

ip igmp snooping maxresponse *vlan-id seconds*

no ip igmp snooping maxresponse *vlan-id*

- *vlan-id* —Number assigned to the VLAN.
- *seconds*—IGMP Maximum response time in seconds. (Range: 1-3174)

Default Configuration

The default maximum response time is 10 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

When using IGMP Snooping Querier, this parameter should be less than the value for the IGMP Snooping Querier query interval.

Example

The following example sets the maximum response time to 60 seconds on VLAN 2.

```
console(config-vlan)#ip igmp snooping maxresponse 2 60
```

ip igmp snooping mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set on a particular VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out (no expiration). The **no** form of this command sets the Multicast Router Present Expiration time to 0. The time is set for a particular VLAN.

Syntax

ip igmp snooping mcrtexpiretime *vlan-id seconds*

no ip igmp mcrtexpiretime *vlan-id*

- *vlan id*—Number assigned to the VLAN
- *seconds*—Multicast router present expiration time. (Range: 1-2147483647)

Default Configuration

The default multicast router present expiration time is 0 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the multicast router present expiration time on VLAN 2 to 60 seconds.

```
console(config-vlan)#ip igmp mcrtexpiretime 2 60
```

14

IGMP Snooping Querier Commands

ip igmp snooping querier

This command enables/disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as source address when generating periodic queries. The **no** form of this command disables IGMP Snooping Querier on the system. Use the optional **address** parameter to reset the querier address to 0.0.0.0.

If a VLAN has IGMP Snooping Querier enabled, and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

The IGMP Snooping Querier application supports the following activities:

- Sends periodic general queries on the VLAN to solicit membership reports

Syntax

ip igmp snooping querier [*vlan-id* [**address** *ipv4_address*]]

no igmp snooping querier [*vlan-id* [**address**]]

- *vlan-id*—A valid VLAN number.
- *ipv4_address*—An IPv4 address.

Default Configuration

IGMP snooping querier is disabled by default.

Command Mode

Global Configuration mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping querier in VLAN Configuration mode.

```
console(config-vlan)#ip igmp snooping querier 1 address 10.19.67.1
```

ip igmp snooping querier query-interval

This command sets the IGMP Querier Query Interval time, which is the amount of time in seconds that the switch waits before sending another general query. The **no** form of this command sets the IGMP Querier Query Interval time to its default value.

Syntax

ip igmp snooping querier query-interval *seconds*

no ip igmp snooping querier query-interval

- *seconds*—Amount of time in seconds that the switch waits before sending another general query. (Range: 1-1800)

Default Configuration

The query interval default is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

The value of this parameter should be larger than the IGMP Snooping Max Response Time.

Example

The following example sets the query interval to 1800:

```
console(config)#ip igmp snooping querier query_interval 1800
```

ip igmp snooping querier timer expiry

This command sets the IGMP Querier timer expiration period which is the time period that the switch remains in Non-Querier mode after it has discovered that there is a Multicast Querier in the network. The **no** form of this command sets the IGMP Querier timer expiration period to its default value.

Syntax

ip igmp snooping querier timer expiry *seconds*

no ip igmp snooping querier timer expiry

- *seconds*—The time in seconds that the switch remains in Non-Querier mode after it has discovered that there is a multicast querier in the network

Default Configuration

The query interval default is 60 seconds.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example sets the querier timer expiry time to 1800 seconds.

```
console(config)#ip igmp snooping querier timer expiry 1800
```

ip igmp snooping querier version

This command sets the IGMP version of the query that the snooping switch is going to send periodically. The **no** form of this command sets the IGMP Querier Version to its default value.

Syntax
ip igmp snooping querier version *number*

no ip igmp snooping querier version

- *number*—IGMP version. (Range: 1–2)

Default Configuration
The querier version default is 2.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example sets the IGMP version of the querier to 1.

```
console(config)#ip igmp snooping querier version 1
```

ip igmp snooping querier election participate

This command enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier source address is more than the Snooping Querier address, it stops sending periodic queries. If the Snooping Querier wins the election, then it

continues sending periodic queries. The **no** form of this command sets the snooping querier not to participate in the querier election but to go into a non-querier mode as soon in as it discovers the presence of another querier in the same VLAN.

Syntax

ip igmp snooping querier election participate *vlan-id*

no ip igmp snooping querier election participate *vlan-id*

Default Configuration

The snooping querier is configured to not participate in the querier election by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the snooping querier to participate in the querier election.

```
console(config-vlan)#ip igmp snooping querier election participate
```

show igmpsnooping querier

This command displays IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

When the optional argument *vlanid* is not used, the command shows the following information:

- Admin Mode —Indicates whether or not IGMP Snooping Querier is active on the switch.
- Admin Version— Indicates the version of IGMP that will be used while sending out the queries.
- Source IP Address—Shows the IP address that is used in the IPv4 header when sending out IGMP queries. It can be configured using the appropriate command.
- Query Interval—Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query
- Querier Timeout—Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following additional information appears:

- VLAN Admin Mode—Indicates whether IGMP Snooping Querier is active on the VLAN.

- VLAN Operational State—Indicates whether IGMP Snooping Querier is in the Querier or Non-Querier state. When the switch is in Querier state it sends out periodic general queries. When in Non-Querier state it waits for moving to Querier state and does not send out any queries.
- VLAN Operational Max Response Time—Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
- Querier Election Participate—Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
- Last Querier Address—Indicates the IP address of the most recent Querier from which a Query was received.
- Last Querier Version—Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.
- Elected Querier—Indicates the IP address of the Querier that has been designated as the Querier based on its source IP address. This field will be 0.0.0.0 when Querier Election Participate mode is disabled

When the optional argument detail is used, the command shows the global information and the information for all Querier enabled VLANs.

Syntax

show ip igmp snooping querier [{**detail** | **vlan** *vlanid*}]

- *vlanid* —Number assigned to the VLAN.

Default Configuration

This command has no default configuration

Command Mode

Privileged Exec mode

User Guidelines

Example

The following example shows querier information for VLAN 2.

```
console#show ip igmp snooping querier vlan 2
```

15

LACP Commands

lacp port-priority

Use the **lacp port-priority** command in Interface Configuration mode to configure the priority value for physical ports. To reset to default priority value, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

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

Default Configuration

The default port priority value is 1.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the priority value for port 1/g8 to 247.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#lacp port-priority 247
```

lacp system-priority

Use the **lacp system-priority** command in Global Configuration mode to configure the Link Aggregation system priority. To reset to default, use the **no** form of this command.

Syntax

lacp system-priority *value*

no lacp system-priority

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

Default Configuration

The default system priority value is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the system priority to 120.

```
console(config)#lacp system-priority 120
```

lacp timeout

Use the **lacp timeout** command in Interface Configuration mode to assign an administrative LACP timeout. To reset the default administrative LACP timeout, use the **no** form of this command.

Syntax

lacp timeout {**long**|**short**}

no lacp timeout

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

Default Configuration

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example assigns an administrative LACP timeout for port 1/g8 to a long timeout value.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#lacp timeout long
```

show lacp ethernet

Use the **show lacp ethernet command in** Privileged EXEC mode to display LACP information for Ethernet ports.

Syntax

show lacp ethernet *interface* [**parameters**|**statistics**]

- *Interface*—Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display LACP Ethernet interface information.

```
console#show lacp ethernet 1/g1
Port 1/g1 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 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 Admin priority:                    0
   port Oper priority:                     0
   port Oper timeout:                      LONG
   LACP Activity:                          ASSIVE
   Aggregation:                            AGGREGATABLE
   synchronization:                        FALSE
   collecting:                             FALSE
   distributing:                           FALSE
   expired:                                FALSE
Port 1/g1 LACP Statistics:
LACP PDUs sent:                            2
LACP PDUs received:                        2
```

show lacp port-channel

Use the **show lacp port-channel** command in Privileged EXEC mode to display LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

- *port_channel_number*—The port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet

Actor
     System Priority:                        1
     MAC Address:                            000285:0E1C00
     Admin Key:                              29
     Oper Key:                               29
Partner
     System Priority:                        0
     MAC Address:                            000000:000000
     Oper Key:                               14
```

16

Link Dependency Commands

link-dependency group

Use the **link-dependency group** command to enter the link-dependency mode to configure a link-dependency group

Syntax

link-dependency group *GroupId*

- *GroupId*—Link dependency group identifier. (Range: 1–16)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

No specific guidelines

Example

```
console(config)#link-dependency group 1
console(config-linkDep-group-1)#
```

no link-dependency group

Use the **no link-dependency group** command to remove the configuration for a link-dependency group.

Syntax

no link-dependency group *GroupId*

- *GroupId*—Link dependency group identifier. (Range: Valid Group Id, 1–16)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

No specific guidelines

Example

```
console(config)#no link-dependency group 1
Configuration cleared for link-dependency group 1
```

add ethernet

Use the **add ethernet** command to add member Ethernet port(s) to the dependency list.

Syntax

add ethernet *intf-list*

- *intf-list*—List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-depend-1)#add ethernet g1
```

no add ethernet

Use the **no add ethernet** command to remove member Ethernet ports from the dependency list.

Syntax

no add ethernet *intf-list*

- *intf-list*—List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Command Mode
Link Dependency mode

Default Configuration
This command has no default configuration.

User Guidelines
No specific guidelines

Example
```
console(config-linkDep-group-1)#no add ethernet g1
```

add port-channel

Use the **add port-channel** command to add member port-channels to the dependency list.

Syntax
add port-channel *port-channel-list*

- *port-channel-list*—List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration
This command has no default configuration.

Command Mode
Link Dependency mode

User Guidelines
No specific guidelines

Example
```
console(config-linkDep-group-1)#add port-channel 2
```

no add port-channel

Use the **no add port-channel** command to remove member port-channels from the dependency list.

Syntax

no add port-channel *port channel list*

- *port-channel-list*—List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#no add port-channel 2
```

depends-on ethernet

Use the **depends-on ethernet** command to add the dependent Ethernet ports list.

Syntax

depends-on ethernet *intf-list*

- *intf-list*—List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#depends-on ethernet g10
```

no depends-on ethernet

Use the **no depends-on ethernet** command to remove the dependent Ethernet ports list.

Syntax

no depends-on ethernet *intf-list*

- *intf-list*—List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#no depends-on ethernet g10
```

depends-on port-channel

Use the **depends-on port-channel** command to add the dependent port-channels list.

Syntax

depends-on port-channel *port-channel-list*

- *port-channel-list*—List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#depends-on port-channel 6
```

no depends-on port-channel

Use the **no depends-on port-channel** command to remove the dependent port-channels list.

Syntax

no depends-on port-channel *port-channel-list*

- *port-channel-list*—List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)# no depends-on port-channel 6
```

show link-dependency

Use the **show link-dependency** command to show the link dependencies configured for a particular group. If no group is specified, then all the configured link-dependency groups are displayed.

Syntax

show link-dependency [*group GroupId*]

- *GroupId*—Link dependency group identifier. (Range: Valid Group Id, 1–16)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

No specific guidelines

Example

The following command shows link dependencies for all groups.

```
console#show link-dependency
GroupId  Member Ports          Ports Depended On
-------  --------------------  ---------------------------------
  2      1/g1-1/g4             1/g8-1/g9
  3      1/g5                  ch2
  5      1/g3-1/g4             1/g10
```

The following command shows link dependencies for group 2 only.

```
console#show link-dependency group 2
GroupId  Member Ports          Ports Depended On
-------  --------------------- ---------------------------------
  2      1/g1-1/g4             1/g8-1/g9
```

17

LLDP Commands

clear lldp remote-data

Use the **clear lldp remote-data** command in Privileged EXEC mode to delete all LLDP information from the remote data table.

Syntax

clear lldp remote-data

Default Configuration

By default, data is removed only on system reset.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to clear the LLDP remote data.

```
console#clear lldp remote-data
```

clear lldp statistics

Use the **clear lldp statistics** command in Privileged EXEC mode to reset all LLDP statistics.

Syntax

clear lldp statistics

Default Configuration

By default, the statistics are only cleared on a system reset.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to reset all LLDP statistics.

```
console#clear lldp statistics
```

lldp notification

Use the **lldp notification** command in Interface Configuration mode to enable remote data change notifications. To disable notifications, use the **no** form of this command.

Syntax

lldp notification

no lldp notification

Default Configuration

By default, notifications are disabled on all supported interfaces.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable remote data change notifications.

```
console(config-if-1/g3)#lldp notification
```

lldp notification-interval

Use the **lldp notification-interval** command in Global Configuration mode to limit how frequently remote data change notifications are sent. To return the notification interval to the factory default, use the **no** form of this command.

Syntax

lldp notification-interval *interval*

no lldp notification-interval

- interval—The smallest interval in seconds at which to send remote data change notifications. (Range: 5 - 3600 seconds)

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to set the interval value to 10 seconds.

```
console(config)#lldp notification-interval 10
```

lldp receive

Use the **lldp receive** command in Interface Configuration mode to enable the LLDP receive capability. To disable reception of LLDPDUs, use the **no** form of this command.

Syntax

lldp receive

no lldp receive

Default Configuration

The default lldp receive mode is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable the LLDP receive capability.

```
console(config-if-1/g3)#lldp receive
```

lldp timers

Use the **lldp timers** command in Global Configuration mode to set the timing parameters for local data transmission on ports enabled for LLDP. To return any or all parameters to factory default, use the **no** form of this command.

Syntax

lldp timers [interval *transmit-interval*] [**hold** *hold-multiplier*] [**reinit** *reinit-delay*]

no lldp timers [interval] [hold] [reinit]

transmit-interval—The interval in seconds at which to transmit local data LLDPDUs. (Range: 1 - 32768 seconds)

hold-multiplier —Multiplier on the transmit interval used to set the TTL in local data LLDPDUs. (Range: 2 - 10)

reinit-delay —The delay in seconds before re-initialization. (Range: 1 - 10 seconds)

Default Configuration

The default transmit interval is 30 seconds.

The default hold-multiplier is 4.

The default delay before re-initialization is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays how to configure LLDP to transmit local information every 1000 seconds.

```
console(config)#lldp timers interval 1000
```

The following example displays how to set the timing parameter at 1000 seconds with a hold multiplier of 8 and a 5 second delay before re-initialization.

```
console(config)#lldp timers interval 1000 hold 8 reinit 5
```

lldp transmit

Use the **lldp transmit** command in Interface Configuration mode to enable the LLDP advertise (transmit) capability. To disable local data transmission, use the **no** form of this command.

Syntax

lldp transmit

no lldp transmit

Default Configuration

LLDP is disabled on all supported interfaces.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how enable the transmission of local data.

```
console(config-if-1/g3)#lldp transmit
```

lldp transmit-mgmt

Use the **lldp transmit-mgmt** command in Interface Configuration mode to include transmission of the local system management address information in the LLDPDUs. To cancel inclusion of the management information, use the **no** form of this command.

Syntax

lldp transmit-mgmt

no lldp transmit-mgmt

Default Configuration

By default, management address information is not included.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to include management information in the LLDPDU.

```
console(config-if-1/g3)#lldp transmit-mgmt
```

lldp transmit-tlv

Use the **lldp transmit-tlv** command in Interface Configuration mode to specify which optional type-length-value settings (TLVs) in the 802.1AB basic management set will be transmitted in the LLDPDUs. To remove an optional TLV, use the **no** form of this command.

Syntax

lldp transmit-tlv [**sys-desc**] [**sys-name**] [**sys-cap**] [**port-desc**]

no lldp transmit-tlv [**sys-desc**] [**sys-name**] [**sys-cap**] [**port-desc**]

- **sys-name**—Transmits the system name TLV
- **sys-desc**—Transmits the system description TLV
- **sys-cap**—Transmits the system capabilities TLV
- **port desc**—Transmits the port description TLV

Default Configuration

By default, no optional TLVs are included.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to include the system description TLV in local data transmit.

```
console(config-if-1/g3)#lldp transmit-tlv sys-desc
```

show lldp

Use the **show lldp** command in Privileged EXEC mode to display the current LLDP configuration summary.

Syntax

show lldp

Default Configuration

This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example displays the current LLDP configuration summary.

```
console# show lldp

Global Configurations:
Transmit Interval: 30 seconds
Transmit TTL Value: 120 seconds
Reinit Delay: 2 seconds
Notification Interval: limited to every 5 seconds

console#show lldp

LLDP transmit and receive disabled on all interfaces
```

show lldp connections

Use the **show lldp connections** command in Privileged EXEC mode to display the current LLDP remote data. This command can display summary information or detail for each interface.

Syntax
show lldp connections [**detail**] [**ethernet** *interface*]

- **detail**—Specifies that a detailed version of remote data is included
- *interface*—Specifies a valid physical interface on the switch or unit/port.

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Examples
The following examples display both the summary information and the detailed information.

Example 1:

```
console#show lldp connections

Local      Remote
Interface  Device ID          Port ID            TTL
---------  -----------------  -----------------  ----------
1/g1       01:23:45:67:89:AB  01:23:45:67:89:AC  60 seconds
1/g2       01:23:45:67:89:CD  01:23:45:67:89:CE  120 seconds
1/g3       01:23:45:67:89:EF  01:23:45:67:89:FG  80 seconds
```

Example 2:

```
console# show lldp connections detail ethernet 1/g1

1/g1 Remote Data:
  Chassis ID: 01:23:45:67:89:AB
  System Name: system-1
  System Description:
  System Capabilities: Bridge
  Port ID: 01:23:45:67:89:AC
  Port Description: port-1
  Management Address: 192.168.112.1
  TTL: 60 seconds
```

show lldp interface

Use the **show lldp interface** command in Privileged EXEC mode to display the current LLDP interface state.

Syntax

show lldp interface {*interface* | **all** }

- *interface*—Specifies a valid physical interface on the switch or unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

This example show how the information is displayed when you use the command with the **all** parameter.

```
console#show lldp interface all

Interface Link Transmit Receive  Notify   TLVs    Mgmt

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

1/g1         Up   Enabled   Enabled  Enabled  0,1,2,3 Y

1/g2         Down Enabled   Enabled  Disabled         Y

1/g3         Down Disabled  Disabled Disabled 1,2     N

TLV Codes: 0 – Port Description, 1 – System Name, 2 – System
Description, 3 –

System Capability

console# show lldp interface 1/g1

Interface Link Transmit Receive  Notify   TLVs    Mgmt

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

1/g1      Up   Enabled  Enabled  Enabled  0,1,2,3 Y

TLV Codes: 0 – Port Description, 1 – System Name, 2 – System
Description, 3 – System Capability
```

show lldp local-device

Use the **show lldp local-device** command in Privileged EXEC mode to display the advertised LLDP local data. This command can display summary information or detail for each interface.

Syntax

show lldp local-device {**detail** *interface* | *interface* | **all**}

- **detail**—includes a detailed version of remote data.
- *interface*—Specifies a valid physical interface on the device, unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

These examples show advertised LLDP local data in two levels of detail.

```
console#show lldp local-device all
LLDP Local Device Summary
Interface Port ID              Port Description
--------- -------------------- --------------------
1/g1      00:62:48:00:00:02

console# show lldp local-device detail 1/g1
LLDP Local Device Detail
Interface: 1/g1
Chassis ID Subtype: MAC Address
Chassis ID: 00:62:48:00:00:00
Port ID Subtype: MAC Address
Port ID: 00:62:48:00:00:02
System Name:
System Description: Routing
Port Description:
System Capabilities Supported: bridge, router
System Capabilities Enabled: bridge
Management Address:
Type: IPv4
Address: 192.168.17.25
```

show lldp remote-device

Use the **lldp remote-device** command in Privileged EXEC mode to display the current LLDP remote data. This command can display summary information or detail for each interface.

Syntax

show lldp remote-device {**detail** *interface* | *interface* | **all**}

- **detail**—Includes detailed version of remote data.
- *interface*—Specifies a valid physical interface on the device, unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

These examples show current LLDP remote data, including a detailed version.

```
console#show lldp remote-device

Local Remote

Interface Device            ID Port           ID TTL

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

1/g1      01:23:45:67:89:AB 01:23:45:67:89:AC 60 seconds

1/g2      01:23:45:67:89:CD 01:23:45:67:89:CE 120 seconds

1/g3      01:23:45:67:89:EF 01:23:45:67:89:FG 80 seconds


console# show lldp remote-device detail 1/g1

Ethernet1/g1,

Remote ID: 01:23:45:67:89:AB

System Name: system-1

System Description:

System Capabilities: Bridge
```

```
Port ID: 01:23:45:67:89:AC
Port Description: 1/g4
Management Address: 192.168.112.1
TTL: 60 seconds
```

show lldp statistics

Use the **show lldp statistics** command in Privileged EXEC mode to display the current LLDP traffic statistics.

Syntax

show lldp statistics {*interface* | **all** }

- *interface*—Specifies a valid physical interface on the switch or unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples shows an example of the display of current LLDP traffic statistics.

```
console#show lldp statistics all

Last Update: Nov 23 2004, 11:09:10

Total Inserts: 15

Total Deletes: 10

Dell Kinnick 1.0 CLI Specification Version 1.6

LVL7 SYSTEMS CONFIDENTIAL 198

Total Drops: 0

Total Ageouts: 5

          Transmit Receive                          TLV      TLV

Interface Total    Total   Discards Errors Ageouts Discards
Unknowns

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

1/g1      10       15      1        0      1       0        0

1/g2      10       8       2        3      4       0        0

1/g3      10       5       0        4      0       0        12
```

The following table explains the fields in this example.

Parameter	Description
Last Update	The value of system of time the last time a remote data entry was created, modified, or deleted.
Total Inserts	The number of times a complete set of information advertised by a remote device has been inserted into the table.
Total Deletes	The number of times a complete set of information advertised by a remote device has been deleted from the table.
Total Drops	The number of times a complete set of information advertised by a remote device could not be inserted due to insufficient resources.
Total Ageouts	The number of times any remote data entry has been deleted due to time-to-live (TTL) expiration.
Transmit Total	The total number of LLDP frames transmitted on the indicated port.
Receive Total	The total number of valid LLDP frames received on the indicated port.
Discards	The number of LLDP frames received on the indicated port and discarded for any reason.
Errors	The number of non-valid LLDP frames received on the indicated port.
Ageouts	The number of times a remote data entry on the indicated port has been deleted due to TTL expiration.
TLV Discards	The number LLDP TLVs (Type, Length, Value sets) received on the indicated port and discarded for any reason by the LLDP agent.
TLV Unknowns	The number of LLDP TLVs received on the indicated port for a type not recognized by the LLDP agent.

18

Password Management Commands

passwords aging

Use the **passwords aging** command in Global Configuration mode to implement expiration date on the passwords. The user is required to change the passwords when they expire.

Use the **no** form of this command to disable the aging function.

Syntax

passwords aging *age*

no passwords aging

- *age*—Time for the expiration of the password. (Range: 1-365 days)

Default Configuration

Password aging is disabled.

Command Mode

Global Configuration mode

User Guidelines

The passwords aging feature functions only if the switch clock is synchronized to an SNTP server. See "Clock Commands" on page 125 for additional information.

Example

The following example sets the password age limit to 100 days.

```
console(config)#passwords aging 100
```

passwords history

As administrator, use the **passwords history** command in Global Configuration mode to set the number of previous passwords that are stored. This setting ensures that users do not reuse their passwords often.

Use the **no** form of this command to disable the password history function.

Syntax

passwords history *historylength*

no passwords history

- *historylength*—Number of previous passwords to be maintained in the history. (Range: 0-10.)

Default Configuration

No password history is maintained.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of previous passwords remembered by the system at 10.

```
console(config)#passwords history 10
```

passwords lock-out

As the administrator, use the **passwords lock-out** command in Global Configuration mode to strengthen the security of the switch by enabling the user lockout feature. When a lockout count is configured, a user who is logging in must enter the correct password within that count. Otherwise that user will be locked out from further switch access. Only an administrator with an access level of 15 can reactivate that user.

Use the **no** form of this command to disable the lockout feature.

Syntax

passwords lock-out *attempts*

no passwords lock-out

- *attempts*—Number of attempts the user is allowed to enter a correct password. (Range: 1-5)

Default Configuration

The user lockout feature is disabled.

Command Mode
Global Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example sets the number of user attempts before lockout at 2.

```
console(config)#passwords lock-out 2
```

passwords min-length

As administrator, use the **passwords min-length** command in Global Configuration mode to enforce a minimum length required for a password. Use the **no** form of this command to disable the password minimum length requirement.

Syntax
passwords min-length *length*

no passwords min-length

- *length*—Required minimum length of the password. (Range: 8–64 characters.)

Default Configuration
Password minimum length is eight characters.

Command Mode
Global Configuration mode.

User Guidelines
This command has no user guidelines.

Example
The following example sets minimum password length to 12 characters.

```
console(config)#passwords min-length 12
```

show passwords configuration

Use the **show passwords configuration** command in Privileged EXEC mode to show the parameters for password configuration.

Syntax

show passwords configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the command output.

```
console#show passwords configuration
passwords configuration:
Minimum password length      : disabled
Minimum password length value: -
Password History             : enabled
Password History length      : 8
aging                        : enabled
aging value                  : 30 days
User lockout                 : enabled
User lockout attempts        : 3
```

19

Port Monitor Commands

monitor session

Use the **monitor session** command in Global Configuration mode to configure a probe port and a monitored port for monitor session (port monitoring). Use the src-interface parameter to specify the interface to monitor. Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an {rx | tx} option, the destination port monitors both ingress and egress packets. Use the destination interface to specify the interface to receive the monitored traffic. Use the mode parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Syntax

monitor session *session-id* {**source interface** *src-interface* [**rx** | **tx**] | **destination interface** *dst-interface* | **mode**}

no monitor session

- *session id*—Session identification number.
- **src-interface**—Ethernet interface (Range: Any valid Ethernet Port)
- **rx**—Monitors received packets only. If no option specified, monitors both rx and tx
- **tx**—Monitors transmitted packets only. If no option is specified, monitors both rx and tx.
- **dst-interface**—Ethernet interface (Range: Any valid Ethernet Port)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following examples shows various port monitoring configurations.

```
console(config)#monitor session 1 source interface 1/g8
console(config)#monitor session 1 destination interface 1/g10
console(config)#monitor session 1 mode
```

show monitor session

Use the **show monitor session** command in Privileged EXEC mode to display status of port monitoring.

Syntax

show monitor session *session-id*

session id—Session identification number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples shows port monitoring status.

```
console#show monitor session 1


Session ID   Admin Mode   Probe Port   Mirrored Port   Type
----------   ----------   ----------   -------------   -----
1            Enable       1/g10        1/g8            Rx,Tx
```

20

PHY Diagnostics Commands

show copper-ports cable-length

Use the **show copper-ports cable-length** command in Privileged EXEC mode to display the estimated copper cable length attached to a port.

Syntax

show copper-ports cable-length [*interface*]

- *interface*—A valid Ethernet port. The full syntax is *unit* / *port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active and working in a 100M or 1000M mode.

Example

The following example displays the estimated copper cable length attached to all ports.

```
console#show copper-ports cable-length

Port     Length [meters]

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

1/g1     <50

1/g2     Copper not active

1/g3     110-140

1/g4     Fiber
```

show copper-ports tdr

Use the **show copper-ports tdr** command in Privileged EXEC mode to display the last Time Domain Reflectometry (TDR)tests on specified ports.

Syntax

show copper-ports tdr [*interface*]

- *interface*—A valid Ethernet port. The full syntax is *unit* / *port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The maximum length of the cable for the Time Domain Reflectometry (TDR) test is 120 meters.

Example

The following example displays the last TDR tests on all ports.

```
console#show copper-ports tdr

Port   Result    Length [meters]      Date

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

1/g1    OK

1/g2    Short     50               13:32:00 23 July 2004

1/g3    Test has not been preformed

1/g4    Open      128              13:32:08 23 July 2004

1/g5    Fiber     -                 -
```

show fiber-ports optical-transceiver

Use the **show fiber-ports optical-transceiver** command in Privileged EXEC mode to display the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [*interface*]

Syntax Description

- *interface*—A valid Ethernet port. The full syntax is *unit* / *port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display the optical transceiver diagnostics.

```
console#show fiber-ports optical-transceiver

Port   Temp    Voltage   Current  Output  Input   TX     LOS
                                    Power           Fault
----------- ------ ------- ------- ------ ------ -----  ---
1/g3   w       OK        E        OK     OK     OK     OK
1/g4   OK      OK        OK       OK     OK     E      OK
1/g1   Copper

Temp - Internally measured transceiver temperature
Voltage - Internally measured supply voltage
Current - Measured TX bias current
Output Power - Measured TX output power in milliWatts
Input Power - Measured RX received power in milliWatts
TX Fault - Transmitter fault
LOS - Loss of signal
```

test copper-port tdr

Use the **test copper-port tdr** command in Privileged EXEC mode to diagnose with Time Domain Reflectometry (TDR) technology the quality and characteristics of a copper cable attached to a port.

Syntax

test copper-port tdr *interface*

- *interface*—A valid Ethernet port. The full syntax is *unit* / *port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines.

During the test shut down the port under test unless it is a combo port with an active fiber port.

NOTE: The maximum distance VCT can function is 120 meters.

Examples

The following example results in a report on the cable attached to port 1/g3.

```
console#test copper-port tdr 1/g3
Cable is open at 64 meters
```

The following example results in a failure to report on the cable attached to port 2/g3.

```
console#test copper-port tdr 2/g3
Can’t perform the test on fiber ports
```

21

System Management Commands

asset-tag

Use the **asset-tag** command in Global Configuration mode to specify the switch asset tag. To remove the existing asset tag, use the **no** form of the command.

Syntax

asset-tag [*unit*] *tag*

no asset-tag [*unit*]

- *unit*—Switch number. (Range: 1–12)
- *tag*—The switch asset tag.

Default Configuration

No asset tag is defined by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the switch asset tag as "1qwepot." Because the unit parameter is not specified, the command defaults to the master switch number.

```
console(config)# asset-tag 1qwepot
```

cut-through mode

Use the **cut-through mode** command to enable the cut-through mode on the switch. The mode takes effect on all ports on next reload of the switch.

Syntax

cut-through mode

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines.

Example

```
console(config)#cut-through mode

The mode (enable) is effective from the next reload of
Switch/Stack.
```

hostname

Use the **hostname** command in Global Configuration mode to specify or modify the switch host name. To restore the default host name, use the **no** form of the command.

Syntax

hostname *name*

no hostname

- *name*—The name of the host. (Range: 1 - 255 characters)

Default Configuration

Host name not configured.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the switch host name.

```
console(config)# hostname Dell
```

ip address

Use the **ip address** command to set a static OOB port IP address.

Syntax

ip address *addr mask gw*

- *addr*—IP address to be set for the OOB port. (Range: Valid IP address)
- *mask*—Subnet mask. (Range: Valid mask)
- *gw*—Gateway IP address. (Range: Valid gateway IP address)

Command Mode

Interface Configuration (out-of-band)

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
console(config-if)#ip address 10.240.4.115 255.255.255.0
10.240.4.1
```

ip address none

Use the **ip address none** command to disable DHCP/BOOTP on the OOB port.

Syntax

ip address none

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (out-of-band)

User Guidelines

No specific guidelines.

Example

```
console(config)#interface out-of-band
```

```
console(config-if)#ip address none
```

ip address

Use the **ip address** command to enable DHCP/BOOTP on the OOB port.

Syntax

ip address {dhcp/bootp}

Command Mode

Interface Configuration (out-of-band)

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
console(config)#interface out-of-band

console(config-if)#ip address dhcp
```

member

Use the **member** command in Stack Global Configuration mode to configure the switch. Execute this command on the Management Switch. To remove a switch from the stack, use the **no** form of the command.

Syntax

member *unit switchindex*

no member *unit*

- *unit* —The switch identifier of the switch to be added or removed from the stack. (Range: 1 - 12)
- *switchindex*—The index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer.

Default configuration

This command has no defaults.

Command Mode

Stack Global Configuration

User Guidelines

The switch index can be obtained by executing the **show supported switchtype** command in User Exec mode.

Example

The following example displays how to add to stack switch number 2 with index 1.

```
console(config)# stack
console(config-stack)# member 2 1
```

movemanagement

Use the **movemanagement** command in Global Configuration mode to move the Management Switch functionality from one switch to another.

Syntax

movemanagement *fromunit tounit*

- *fromunit*—The switch identifier on the current Management Switch.
- *tounit*—The switch identifier on the new Management Switch.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Upon execution, the entire stack, including all interfaces in the stack, are unconfigured and reconfigured with the configuration on the new Management Switch.

After the reload is complete, all stack management capability must be performed on the new Management Switch.

To preserve the current configuration across a stack move, execute the **copy** configuration command before performing the stack move. A stack move causes all routes and layer 2 addresses to be lost. This command is executed on the Management Switch. The administrator is prompted to confirm the management move.

Example

The following example displays how to move the Management Switch functionality from switch "1" to switch "8."

```
console(config)#stack

console(config)#movemanagement 1 2
```

no cut-through mode

Use the **no cut-through mode** command to disable the cut-through mode on the switch. The command takes effect on all ports on next reload of the switch.

Syntax

no cut-through mode

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines.

Example

```
Console(config)#no cut-through mode

The mode (disable) is effective from the next reload of
Switch/Stack.
```

no standby

Use the **no standby** command to unconfigure the standby in the stack. In this case, FASTPATH automatically selects a standby from the existing stack units.

Syntax

no standby

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration

User Guidelines

No specific guidelines.

Example

```
console(config)#stack

console(config-stack)#no standby

Fastpath will automatically select a standby
```

ping

Use the **ping** command in User EXEC mode to check the accessibility of the desired node on the network.

Syntax

ping {*ip-address* |*hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*] | ipv6}

- *ip-address* —IP address to ping (contact).
- *Hostname*—Hostname to ping (contact). (Range: 1 - 158 characters)
- *packet_size*—Number of bytes in a packet. (Range: 56 - 1472 bytes) The actual packet size is eight bytes larger than the size specified because the switch adds header information.
- *packet_count*—Number of packets to send. (Range: 1 - 65,535 packets)
- *time_out*—Timeout in milliseconds to wait for each reply. (Range: 50 - 65,535 milliseconds)

Default Configuration

The default packet size is 64 bytes.

The default packet count is 4 packets.

The default time-out is 2000 milliseconds.

Command Mode

User EXEC mode

User Guidelines

If the packet count is not specified, the packet count defaults to four pings.

Following are sample results of the **ping** command:

- *Destination does not respond*—If the host does not respond, a "No answer from host" message appears in 10 seconds.

- *Destination unreachable*—The gateway for this destination indicates that the destination is unreachable. In such cases, the "Host unreachable" message appears.
- *Network or host unreachable*—The switch found no corresponding entry in the route table. In such cases the "Network or Host unreachable" message appears.

Examples

The following example displays a ping to IP address 10.1.1.1.

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

The following example displays a ping to yahoo.com.

```
console#ping yahoo.com
Pinging yahoo.com [66,217,71,198] 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
```

reload

Use the **reload** command in Privileged EXEC mode to reload stack members.

Syntax

reload [*unit*]

- *unit* —Unit number to be reloaded.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If no unit is specified, all units are reloaded.

Example

The following example displays how to reload the stack.

```
console#reload 1

Management switch has unsaved changes.
Would you like to save them now? (y/n)n
Configuration Not Saved!
Are you sure you want to reload the switch? (y/n) y
Reloading management switch 1.
```

set description

Use the **set description** command in Stack Global Configuration mode to associate a text description with a switch in the stack.

Syntax

set description *unit description*

- *unit*—The switch identifier.
- *description*—The text description. (Range: 1 - 80 alphanumeric characters)

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays

```
console(config)#stack

console(config-stack)#set description 1 "unit 1"
```

show boot-version

Use the **show boot-version** command to display the boot image version details. The details available to the user include the build date and time.

Syntax

show boot-version

Default Configuration

This command has no default configuration.

Command Mode

User EXEC or Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
console#show boot-version

unit          Boot Image Version
1             Thu Aug 30 12:01:04 2007
```

show cut-through mode

Use the **show cut-through mode** command to show the cut-through mode on the switch.

Syntax

show cut-through mode

Command Mode

Privileged EXEC

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
Console#show cut-through mode

Current mode    : Enable

Configured mode : Disable (This mode is effective on next reload)
```

show ip interface out-of-band

Use the **show ip interface out-of-band** command to disable DHCP/BOOTP on the OOB port.

Syntax

show ip interface out-of-band

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
console#show ip interface out-of-band


IP Address..........................  10.240.4.115

Subnet Mask.........................  255.255.255.0

Default Gateway.....................  10.240.4.1

IPv6 Prefix is .....................  FE80::20A:1EFF:FE11:1100/64

ServPort Configured Protocol Current...None

Burned In MAC Address.................0006.2932.814C
```

show memory cpu

Use the **show memory cpu** command to check the total and available RAM space on the switch.

Syntax

show memory cpu

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
console#show memory cpu


Total Memory..................................... 262144 KBytes
Available Memory Space........................... 121181 KBytes
```

show process cpu

Use the **show process cpu** command to check the CPU utilization for each process currently running on the switch.

Syntax

show process cpu

Command Mode

Privileged EXEC

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
console#show process cpu
Memory Utilization Report
status   bytes
------   ----------
Free     27896864
Alloc  168268448

Task Utilization Report
Task                     Utilization
------------------------ -----------
osapiTimer               1.10%
bcmL2X.0                 0.80%
bcmCNTR.0                0.30%
bcmLINK.0                0.45%
bcmRX                    14.95%
dtlTask                  2.50%
hapiRxTask               2.95%
RMONTask                 0.05%
ipMapForwardingTask      18.30%
IGMP                     0.05%
Kernel/Interrupt/Idle    58.55%

Total                    100.00%
```

show sessions

Use the **show sessions** command in Privileged EXEC mode to display a list of the open telnet sessions to remote hosts.

Syntax

show sessions

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a list of open telnet sessions to remote hosts.

```
console#show sessions

Connection        Host          Address        Port

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

1             Remote switch     172.16.1.1     23

2             172.16.1.2        172.16.1.2     23
```

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

Field	Description
Connection	Connection number
Host	Remote host to which the switch is connected through a Telnet session
Address	IP address of the remote host
Port	Telnet TCP port number

show stack-port

Use the **show stack-port** command in Privileged EXEC mode to display summary stack-port information for all interfaces.

Syntax

show stack-port

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the summary stack-port.

```
console#show stack-port

.............. .Configured Running
                 Stack      Stack     Link      Link
Unit  Interface  Mode       Mode      Status    Speed (Gb/s)
----  ---------  ----------  --------  --------  ------------
1      xg1       Stack      Stack     Link Down   12
1      xg2       Stack      Stack     Link Down   12
1      xg3       Ethernet   Ethernet  Link Down   10
1      xg4       Ethernet   Ethernet  Link Down   10
```

The following table explains the fields in the example.

Field	Description
Interface	Unit/Port
Configured Stack Mode	Stack or Ethernet
Running Stack Mode	Stack of Ethernet

Field	Description
Link Status	Status of the link
Link Speed	Speed (Gb/sec) of the stack port link

show stack-port counters

Use the **show stack-port counters** command in Privileged EXEC mode to display summary data counter information for all interfaces.

Syntax

show stack-port counters

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the summary stack-port counters.

```
console#show stack-port counters

------------TX-------------- ------------RX--------------

                 Data    Error              Data  Error

                 Rate    Rate       Total   Rate  Rate       Total

Unit Interface   (Mb/s)  (Errors/s) Errors  (Mb/s)Errors/s)  Errors

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

1    xg1         0       0          0       0     0          0

1    xg2         0       0          0       0     0          0

1    xg3         0       0          0       0     0          0

1    xg4         0       0          0       0     0          0
```

The following table describes the fields in the example.

Field	Description
Unit	Unit
Interface	Port
Tx Data Rate	Transmit data rate in megabits per second on the stacking port.
Tx Error Rate	Platform-specific number of transmit errors per second.
Rx Data Rate	Receive data rate in megabits per second on the stacking port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.

show stack-port diag

NOTE: This command is intended only for Field Application Engineers (FAE) and developers. An FAE will advise when to run this command and capture this information.

Use the **show stack-port diag** command in Privileged EXEC mode to display front panel stacking diagnostics for each port.

Syntax

show stack-port diag

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the front panel stacking diagnostics.

```
console#show stack-port diag

1/xg1:

RBYT:0 RPKT:0 TBYT:e38b50 TPKT:d1ba

RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0

console#show stack-port diag

1/xg2:

RBYT:0 RPKT:0 TBYT:e38b50 TPKT:d1ba

RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0


Legend:

RBYT : Received Bytes

RPKT : Received Packets

TBYT : Transmitted Bytes

TPKT : Transmitted Packets
```

```
RFCS : Received Frame Check Sequence Errors
RFRG : Received Fragment Errors
RJBR : Received Jabber Errors
RUND : Received Underrun Errors
ROVR : Received Overrun Errors
TFCS : Transmit Frame Check Sequence Errors
TERR : Transmit Errors

1 - xg1:
RBYT:148174422 RPKT:528389 TBYT:679827058 TPKT:2977561
RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0
TFCS:0 TERR:0

1 - xg2:
RBYT:0 RPKT:0 TBYT:419413311 TPKT:620443
RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0
TFCS:0 TERR:0
```

The following table describes the fields in the example.

Field	Description
Interface	Port
Diagnostic Entry 1	80 character string used for diagnostics
Diagnostic Entry 2	80 character string used for diagnostics
Diagnostic Entry 3	80 character string used for diagnostics

show stack standby

Use the **show stack-standby** command to show the Standby configured in the stack. The **show stack-standby** command shows the configured or automatically selected standby unit number.

Syntax

show stack-standby

Default Configuration

This command has no default configuration.

Command Mode

privileged EXEC or User EXEC

User Guidelines

No specific guidelines.

Example

```
console>show stack-standby

standby unit: 3
```

show supported switchtype

Use the **show supported switchtype** command in User EXEC mode to display information about all supported switch types.

Syntax

show supported switchtype [*switchindex*]

- *switchindex*—Specifies the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. (Range: 0 - 65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the information for supported switch types.

```
console>show supported switchtype

                                          Mgmt      Code
SID         Switch Model ID               Pref      Type
--- -------------------------------- -----------  --------
1   M6220 Disabled     0x100b000
```

The following table describes the fields in the example.

Field	Description
Switch Index (SID)	This field displays the index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	This field displays the model identifier for the supported switch type.
Management Preference	This field indicates the management preference value of the switch type.
Code Version	This field displays the code load target identifier of the switch type.

The following example displays the format of the **show supported switchtype** [*switchindex*] command.

```
console#show supported switchtype 1

Switch Type..................... 0x73950001

Model Identifier................ PCTM6220

Switch Description.............. PowerConnect M6220

Management Preference........... 1

Expected Code Type.............. 0x100b000

Supported Cards:

   Card Index (CID)............. 3

   Model Identifier............. PCT6224
```

The following table describes the fields in the example.

Field	Description
Switch Type	This field displays the 32-bit numeric switch type for the supported switch.
Model Identifier	This field displays the model identifier for the supported switch type.
Switch Description	This field displays the description for the supported switch type.

show switch

Use the **show switch** command in User EXEC mode to display information about all units in the stack. Use the **show switch** [*unit*] command to display the information about a specific unit on the stack.

Syntax

show switch [*unit*]

- *unit*—The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays stack status information for the switch.

```
console>show switch 1

Switch.............................. 1

Management Status................... Management Switch

Admin Management Preference....... 4

Switch Type......................... 0x73950001

Preconfigured Model Identifier.... PCT6224

Plugged-in Model Identifier....... PCT6224

Switch Status....................... OK

Switch Description................. PCT6224

Expected Code Type................. 0x100b000

Detected Code Version.............. I.12.21.1

Detected Code in Flash............. I.12.21.1

Boot Code Version.................. I.12.1

Up Time............................. 1 days 0 hrs 16 mins 37 secs
```

The following table describes the fields in the example.

Unit	Description
Switch	This field displays the unit identifier assigned to the switch.
Management Status	This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.
Admin Management Preference	This field indicates the administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Management Switch.
Switch Type	This field displays the 32-bit numeric switch type.
Model Identifier	This field displays the model identifier for this switch. Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Switch Status	This field displays the switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present.
Switch Description	This field displays the switch description.
Expected Code Version	This field indicates the expected code version.
Detected Code Version	This field displays the version of code running on this switch. If the switch is not present and the data is from preconfiguration, the code version is "None."
Detected Code in Flash	This field displays the version of code that is currently stored in FLASH memory on the switch. This code will execute after the switch is reset. If the switch is not present and the data is from pre-configuration, then the code version is "None."
Boot Code Version	This field displays the version of the boot strapping code.
Up Time	This field displays the system up time.

This example displays information about all units in the stack.

```
console>show switch

Switch   Management   Preconfig   Plugged-in   Switch   Code
         Status       Model ID    Model ID     Status   Version

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

1        Mgmt Switch  PCT6224     PCT6224              1.12.21.1
```

Different fields in the display are explained as follows:

Unit	Description
Switch	This field displays the unit identifier assigned to the switch.
Management Status	This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.
Preconfigured Model Identifier	This field displays the model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Plugged-In Model Identifier	This field displays the model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Switch Status	This field indicates the switch status. Possible values for this state are: OK, Unsupported, CodeMismatch, ConfigMismatch, or NotPresent
Code Version	This field indicates the detected version of code on this switch.

show system

Use the **show system** command in User EXEC mode command to display system information.

Syntax

show system [*unit*]

- *unit*—The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system information.

```
console>show system
System Description: Ethernet switch
System Up Time (days,hour:min:sec): 1,22:38:21
System Contact:
System Name: RS1
System location:
System MAC Address: 00:10:B5:F4:00:01
Sys Object ID: 1.3.6.1.4.1.674.10895.3004
Type: PowerConnect 6424
Temperature Sensors:
Unit     Sensor     Temperature       Status
                     (Celsius)
------   -------    -------------     --------
1        1          41                OK
1        2          41                OK
2        1          42                OK
2        2          42                OK
Unit    Power supply    Source        Status
------  ------------    ---------     -------
1       Main            AC            OK
2       Secondary       AC            OK
Unit     FAN      Status
------   ------   -------
1        CPU      OK
2        CPU      OK
```

show system id

Use the **show system id** command in User EXEC mode to display the system identity information.

Syntax

show system id [*unit*]

- *unit*—The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

The tag information is on a switch by switch basis.

Example

The following example displays the system service tag information.

```
console>show system id

Service Tag: 89788978

Serial number: 8936589782

Asset tag: 7843678957

Unit    Service tag     Serial number     Asset tag
-----   ------------    --------------    -----------
1       89788978        8936589782        7843678957
2       4254675         3216523877        5621987728
```

show users

Use the **show users** command in Privileged EXEC mode to display information about the active users.

Syntax

show users

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a list of active users and the information about them.

```
console#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
```

show version

Use the **show version** command in User EXEC mode to displays the system version information.

Syntax

show version [*unit*]

- *unit*—The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a system version (this version number is only for demonstration purposes).

```
console>show version

Image Descriptions

image1 : default image

image2 :

Images currently available on Flash

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

unit    image1     image2     current-active    next-active

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

1       K.3.9.1    0.0.0.0    image1            image1

2       K.3.9.1    0.0.0.0    image1            image1
```

stack

Use the **stack** command in Global Configuration mode to set the mode to Stack Global Config.

Syntax

stack

Default Configuration

This command has no default mode.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the mode to Stack Global Config.

```
console(config)#stack

console(config-stack)#
```

standby

Use the **standby** command to configure the standby in the stack. This unit comes up as the master when the stack failover occurs. Use the **no** form of this command to reset to default, in which case, FASTPATH automatically selects a standby from the existing stack units if there no preconfiguration.

Syntax

standby *unit*

- *unit*—Valid unit number in the stack. (Range: 1–12 maximum. The range is limited to the number of units available on the stack.)

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration

User Guidelines

No specific guidelines.

Examples

```
console(config)#stack

console(config-stack)#standby 2
```

switch priority

Use the **switch priority** command in Global Configuration mode to configure the ability of the switch to become the Management Switch. The switch with the highest priority value is chosen to become the Management Switch if the active Management Switch fails.

Syntax

switch *unit* **priority** *value*

- *unit*—The switch identifier. (Range: 1 - 12)
- *value*—The priority of one backup switch over another. (Range: 0 - 12)

Default Configuration

The switch priority defaults to the hardware management preference value of 1.

Command Mode

Global Configuration mode

User Guidelines

Switches that do not have the hardware capability to become the Management Switch are not eligible for management.

Example

The following example displays how to configure switch number "1" to have a priority of "2" for becoming the Management Switch.

```
console(config)#switch 1 priority 2
```

switch renumber

Use the **switch renumber** command in Global Configuration mode to change the identifier for a switch in the stack. Upon execution, the switch is configured with the configuration information for the new switch, if any is available. The old switch configuration information is retained; however, the old switch will be *operationally unplugged*.

Syntax

switch *oldunit* **renumber** *newunit*

- *oldunit*—The current switch identifier. (Range: 1 - 12)
- *newunit*—The updated value of the switch identifier. (Range: 1 - 12)

Command Modes

Global Configuration mode

User Guidelines

This command is executed on the Management Switch.

Example

The following example displays how to reconfigure switch number "1" to an identifier of "2."

```
console(config)#switch 1 renumber 2
```

telnet

Use the **telnet** command in Privileged EXEC mode to log into a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword1*.....]

- *ip-address* — Valid IP address of the destination host.
- *hostname* — Hostname of the destination host. (Range: 1 - 158 characters)

- *port* — A decimal TCP port number, or one of the keywords from the port table in the usage guidelines (see Port Table).
- *keyword* — One or more keywords from the keywords table in the user guidelines (see Keywords Table).

Default Configuration

port — Telnet port (decimal 23) on the host.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#telnet 1.1.1.1?
```

Keywords Table

Options	Description
debug	Enable telnet debugging mode.
line	Enable telnet linemode.
noecho	Disable local echo.
<cr>	Press ENTER to execute the command.
<port>	Enter the port number.

Port Table

Keyword	Description	Port Number
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37

Keyword	Description	Port Number
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example

Following is an example of using the **telnet** command to connect to 176.213.10.50.

```
console#telnet 176.213.10.50

Esc U sends telnet EL
```

traceroute

Use the **traceroute** command in Privileged EXEC mode to discover the IP routes that packets actually take when traveling to their destinations.

You can use **traceroute** command in either of two formats:

- You can specify the IP address and hostname in the command. The **traceroute** {ipaddress|hostname} command sets the parameters to their default values.
- You can enter **traceroute** to without specifying the IP address and hostname, and specify values for the traceroute parameters.

Syntax

Use the following command form to specify the IP address and hostname in the command line:

traceroute {ipaddress|hostname}

- *ip-address* — Valid IP address of the destination host.
- *hostname* — Hostname of the destination host. (Range: 1 - 158 characters)

Or, use the following command form to initiate an iterative process of setting the parameters.

traceroute

This command interactively takes user inputs for the following parameters.

- *ip-address* — Valid IP address of the destination host.
- *hostname* — Hostname of the destination host. (Range: 1 - 158 characters)
- *packet_size* — Number of bytes in a packet. (Range: 40-1500)
- *max-ttl* — The largest TTL value that can be used. The **traceroute** User EXEC command terminates when the destination is reached or when this value is reached. (Range:1- 255)
- *packet_count* — The number of probes to be sent at each TTL level. (Range:1-10)

- *time_out* — The number of seconds to wait for a response to a probe packet. (Range: 1- 60)
- *ip-address*— One of the interface addresses of the switch to use as a source address for the probes. The switch picks the valid IP address it considers to be the best source address to use.
- *tos*— The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

Default Configuration

packet_size — The default is 40 bytes.

max-ttl — The default is 20.

packet_count — The default count is 3.

time_out — The default is 3 seconds.

Command Mode

Privileged EXEC mode

User Guidelines

This command works by taking advantage of the error messages generated by switches when a datagram exceeds its time-to-live (TTL) value. The **traceroute** command terminates when the destination responds when the maximum TTL is exceeded.

Examples

The following example discovers the routes that packets will actually take when traveling to the destination specified in the command.

```
console#traceroute 192.168.77.171

Tracing route over a maximum of 20 hops

 1  192.168.21.1       30 ms      10 ms      10 ms

 2                      *          *          *

 3                      *          *          *

 4                      *          *          *

 5                      *          *          *
```

The following example uses the iterative process to obtain command parameters, and displays the routes that packets actually take when traveling to their destination.

```
console#traceroute

traceroute# Enter the ip-address|hostname : 192.168.77.171

traceroute# Packet size (default: 40 bytes): 30

traceroute# Max ttl value (default: 20):  10

traceroute# Number of probes to send at each level (default 3):

traceroute# Timeout (default: 3 seconds): 6

traceroute# Source ip-address (default to select best interface
address):

traceroute# Type of Service byte (default):

Tracing route over a maximum of 20 hops

1 192.168.21.1   30 ms   10 ms    10 ms
2                *        *        *
3                *        *        *
4                *        *        *
5                *        *        *
```

22

ACL Commands

access-list

Use the **access-list** command in Global Configuration mode to create an Access Control List (ACL) that is identified by the parameter *list-name*.

Syntax

access-list *std-list-num* {**deny** | **permit**} {*srcip srcmask* | **every**} [**log**] [**assign-queue** *queue-id*] [**redirect** *interface* | **mirror** *interface*]

access-list *ext-list-num* {**deny** | **permit**} {**every** | {[**icmp** | **igmp** | **ip** | **tcp** | **udp** | **number**] {*srcip srcmask* | **any**} [**eq** [*portkey* | *portvalue*]] {**dstip** *dstmask* | **any**} [**eq** [**portkey** | **portvalue**]] [**precedence** *precedence* | **tos** *tos tosmask* | **dscp** *dscp*] [log] [**assign-queue** *queue-id*] [**redirect** *interface* | **mirror** *interface*]}}

no access-list *list-name*

- *list-name*—Access-list name up to 31 characters in length.
- **deny | permit**—Specifies whether the IP ACL rule permits or denies an action.
- **every**—Allows all protocols.
- **eq**—Equal. Refers to the Layer 4 port number being used as match criteria. The first reference is source match criteria, the second is destination match criteria.
- *number*—Standard protocol number. Protocol keywords icmp,igmp,ip,tcp,udp.
- *srcip*—Source IP address.
- *srcmask*—Source IP mask.
- *dstip*—Destination IP address.
- *dstmask*—Destination IP mask.
- *portvalue*—The source layer 4 port match condition for the ACL rule is specified by the port value parameter (Range: 0 - 65535).
- *portkey*—Or you can specify the *portkey*, which can be one of the following keywords: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.

- **log**—Specifies that this rule is to be logged.
- **assign-queue** *queue-id*—Specifies the particular hardware queue for handling traffic that matches the rule. (Range: 0-6)
- **mirror** *interface*—Allows the traffic matching this rule to be copied to the specified interface.
- **redirect** *interface*—This parameter allows the traffic matching this rule to be forwarded to the specified unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Users are permitted to add rules, but if a packet does not match any user-specified rules, the packet is dropped by the implicit "deny all" rule.

Examples

The following examples create an ACL to discard any HTTP traffic from 192.168.77.171, but allow all other traffic from 192.168.77.171:

```
console(config)#access-list alpha deny 192.168.77.171 0.0.0.0
0.0.0.0 255.255.255.255 eq http

console(config)#access-list alpha permit 192.168.77.171 0.0.0.0
```

deny | permit

Use the **deny** command in Mac-Access-List Configuration mode to deny traffic if the conditions defined in the deny statement are matched. Use the **permit** command in Mac-Access-List Configuration mode to allow traffic if the conditions defined in the permit statement are matched.

Syntax

{**deny | permit**} {*srcmac srcmacmask* | **any**} {*dstmac dstmacmask* | **any | bpdu** } [{*ethertypekey* | *0x0600-0xFFFF* }] [**vlan eq** *0-4095*] [**cos** *0-7*] [**secondary-vlan eq** *0-4095*] [**secondary-cos** *0-7*] [**log**] [**assign-queue** *queue-id*] [{**mirror |redirect**} *interface*]

- *srcmac*—Valid source MAC address in format xxxx.xxxx.xxxx.
- *srcmacmask*—Valid MAC address bitmask for the source MAC address in format xxxx.xxxx.xxxx.
- **any**—Packets sent to or received from any MAC address

- *dstmac*—Valid destination MAC address in format xxxx.xxxx.xxxx.
- *destmacmask*—Valid MAC address bitmask for the destination MAC address in format xxxx.xxxx.xxxx.
- **bpdu**—Bridge protocol data unit
- *ethertypekey*—Either a keyword or valid four-digit hexadecimal number. (Range: Supported values are appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, Netbios, novell, pppoe, rarp.)
- *0x0600-0xFFFF*—Specify custom ethertype value (hexadecimal range 0x0600-0xFFFF)
- **vlan eq**—VLAN number. (Range 0-4095)
- **cos**—Class of service. (Range 0-7)
- **secondary-vlan eq**—Secondary VLAN number. (Range 0-4095)
- **secondary-cos**—Secondary class of service. (Range 0-7)
- **log**—Specifies that this rule is to be logged.
- **assign-queue**—Specifies particular hardware queue for handling traffic that matches the rule.
- *queue-id*—0-6, where n is number of user configurable queues available for that hardware platform.
- **mirror**—Copies the traffic matching this rule to the specified interface.
- **redirect**—Forwards traffic matching this rule to the specified physical interface.
- *interface*—Valid physical interface in *unit/<port-type>port* format, for example 1/g12.

Default Configuration

This command has no default configuration.

Command Mode

Mac-Access-List Configuration mode

User Guidelines

The **no** form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather the entire ACL must be deleted and re-specified.

The assign-queue and redirect parameters are only valid for permit command s.

Example

The following example configures a MAC ACL to deny traffic from MAC address 0806.c200.0000.

```
console(config)#mac access-list extended DELL123
console(config-mac-access-list)#deny 0806.c200.0000 ffff.ffff.ffff
any
```

ip access-group

no ip access-group

Use the **ip access-group** or **no ip access-group** command to apply/disable an IP based egress ACL on an Ethernet interface or a group of interfaces. An IP based ACL should have been created by the **access-list** <*name*> … command with the same name specified in this command.

Syntax

ip access-group *name direction*

- *name*—Access list name. (Range: Valid IP access-list name up to 31 characters in length)
- *direction*—Direction of the ACL. (Range: In or out)

Default Configuration

This command has no default configuration.

Command Mode

Global and Interface Configuration

User Guidelines

Global mode command configures the ACL on all the interfaces, whereas the interface mode command does so for the interface.

Examples

```
console(config)#ip access-group aclname in
console(config)#no ip access-group aclname in
console(config)#ip access-group aclname1 out
console(config-if-1/g1)#ip access-group aclname out
console(config-if-1/g1)#no ip access-group aclname out
```

mac access-group

Use the **mac access-group** command in Global Configuration or Interface Configuration mode to attach a specific MAC Access Control List (ACL) to an interface in a given direction.

Syntax

mac access-group *name sequence*

no mac access-group *name*

- *name*—Name of the existing MAC access list. (Range: 1-31 characters)
- *sequence*—Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, VLAN or Port Channel) mode

User Guidelines

An optional sequence number may be specified to indicate the order of this access-list relative to the other access-lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number already is in use for this interface and direction, the specified access-list replaces the currently attached access list using that sequence number. If the sequence number is not specified for this command, a sequence number is selected that is one greater than the highest sequence number currently in use for this interface and direction.

This command specified in Interface Configuration mode only affects a single interface.

Example

The following example assigns a MAC access group to port 1/g1 with the name DELL123.

```
console(config)#interface 1/g1

console(config-if-1/g1)#mac access-group DELL123
```

mac access-list extended

Use the **mac access-list extended command** in Global Configuration mode to create the MAC Access Control List (ACL) identified by the *name* parameter.

Syntax

mac access-list extended *name*

no mac access-list extended *name*

- *name* —Name of the access list. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to create a mac access control list. The CLI mode is changed to Mac-Access-List Configuration when this command is successfully executed.

Example

The following example creates MAC ACL and enters MAC-Access-List-Configuration mode.

```
console(config)#mac access-list extended LVL7DELL
console(config-mac-access-list)#
```

mac access-list extended rename

Use the **mac access-list extended rename** command in Global Configuration mode to rename the existing MAC Access Control List (ACL).

Syntax

mac access-list extended rename *name newname*

- *name* —Existing name of the access list. (Range: 1-31 characters)
- *newname*—New name of the access list. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Command fails if the new name is the same as the old one.

Example

The following example shows the **mac access-list extended rename** command.

```
console(config)#mac access-list extended rename DELL1 DELL2
```

show ip access-lists

Use the **show ip access-lists** command in Privileged EXEC mode to display access lists applied on interfaces and all rules that are defined for the access lists.

Syntax

show ip access-lists *accesslistname*

- *accesslistname*—The name used to identify the ACL. The range is 1-31 characters.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays IP ACLs configured on a device.

```
console#show ip access-lists
Current number of ACLs: 2  Maximum number of ACLs: 100

   ACL Name             Rules      Interface(s)         Vlan(s)
----------------------- ------ ------------------------ --------
ACL40                    1
ACL41                    1
```

show mac access-list

Use the **show mac access-list** command in Privileged EXEC mode to display a MAC access list and all of the rules that are defined for the ACL.

Syntax

show mac access-list *name*

- *name*—Identifies a specific MAC access list to display.

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a MAC access list and all associated rules.

```
console#show mac access-list DELL123
```

The command output provides the following information:

Field	Description
MAC ACL Name	The name of the MAC access list.
Rules	The number of user-configured rules defined for the MAC ACL. The implicit 'deny all' rule defined at the end of every MAC ACL is not included.
Interfaces	Displays the list of interfaces (unit/port) to which the MAC ACL is attached in a given direction.

23

Line Commands

exec-timeout

Use the **exec-timeout** command in Line Configuration mode to set the interval that the system waits for user input before timeout. To restore the default setting, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

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

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

To specify no timeout, enter the **exec-timeout 00** command.

Example

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

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

history

Use the **history** command in Line Configuration mode to enable the command history function. To disable the command history function, use the **no** form of this command.

Syntax

history

no history

Default Configuration

The default value for this command is *enabled*.

Command Mode

Line Interface mode

User Guidelines

This command has no user guidelines.

Example

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

```
console(config-line)# no history
```

history size

Use the **history size** command in Line Configuration mode to change the command history buffer size for a particular line. To reset the command history buffer size to the default setting, use the **no** form of this command.

Syntax

history size *number-of-commands*

no history size

- *number-of-commands*—Specifies the number of commands the system may record in its command history buffer. (Range: 0-216)

Default Configuration

The default command history buffer size is 10.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

```
console(config-line)#history size 20
```

line

Use the **line** command in Global Configuration mode to identify a specific line for configuration and enter the line configuration command mode.

Syntax

line {console|telnet|ssh}

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

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following example enters Line Configuration mode to configure Telnet.

```
console(config)#line telnet

console(config-line)#
```

show line

Use the **show line** command in User EXEC mode to display line parameters.

Syntax

show line [console|telnet|ssh]

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

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the line configuration.

```
console>show line
Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1
Telnet configuration:
Interactive timeout: 10 minutes 10 seconds
History: 10
SSH configuration:
Interactive timeout: 10 minutes 10 seconds
History: 10
```

speed

Use the **speed** command in Line Configuration mode to set the line baud rate. Use the **no** form of the command to restore the default settings.

Syntax

speed {*bps*}

no speed

- *bps*—Baud rate in bits per second (bps). The options are 2400, 9600, 19200, 38400, 57600, and 115200.

Default Configuration

This default speed is 9600.

Command Mode

Line Interface (console) mode

User Guidelines

This configuration applies only to the current session.

Example

The following example configures the console baud rate to 9600.

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

24

IP Addressing Commands

clear host

Use the **clear host** command in Privileged EXEC mode to delete entries from the host name-to-address cache.

Syntax

clear host {*name*|*}

- *name*—Host name to be deleted from the host name-to-address cache. (Range: 1-255 characters)
- *—Deletes all entries in the host name-to-address cache.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#clear host *
```

helper-address

Use the **helper-address** command in Interface Configuration mode to enable forwarding User Datagram Protocol (UDP) Broadcast packets received on an interface. To disable forwarding Broadcast packets to specific addresses, use the no form of this command.

Syntax

helper-address *ip-address* [*udp-port-list*]

no helper-address *ip-address*

- *ip-address*—Destination broadcast or host address to be used when forwarding UDP broadcasts. Specify 0.0.0.0 to indicate not to forward the UDP packet to any host.
- *udp-port-list*—The broadcast packet destination UDP port number to forward. If not specified, packets for the default services are forwarded to the helper address. (Range: 0-65535, comma delimited, e.g. 80,100)

Default Configuration

Broadcast packets forwarding to specific addresses is disabled. 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)

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Many helper addresses can be defined. The maximum number of address-port pairs is up to 128 for the whole device.

The helper-address interface configuration command forwards a specific UDP Broadcast from one interface to another.

The helper-address interface configuration command specifies a UDP port number for which UDP Broadcast packets with that destination port number are forwarded.

The helper-address interface configuration command does not enable forwarding packets using BOOTP/DHCP. To forward packets using BOOTP/DHCP, use the **bootpdhcprelay enable** and **bootpdhcprelay serverip** Global Configuration commands and the **show bootpdhcprelay** Privileged EXEC command.

Example

The following example specifies UDP helper address. UDP packets are forwarded to helper address.

```
console(config-vlan1)#helper-address 131.108.1.27 30,100-120,201
```

interface out-of-band

Use the **interface out-of-band** command to bring up the OOB port configuration menu.

Syntax Description

interface out-of-band

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines.

Example

```
console(config)#interface out-of-band

console(config-if)#
```

ip address

Use the **ip address** command in Global Configuration mode to set an IP address. To remove an IP address, use the **no** form of this command.

Syntax

ip address *ip-address* {*mask* |*prefix-length*}

no ip address

- *ip-address*—Specifies a valid IP address.
- *mask*—Specifies a valid subnet (network) mask IP address.
- *prefix-length*—The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 1-30)

Default Configuration

No IP address is defined for the switch management interface.

Command Mode

Global Configuration mode

User Guidelines

IP address protocol should be set to none before setting the static IP address.

Examples

The following examples configure the IP address 131.108.1.27 and subnet mask 255.255.255.0 and the same IP address with prefix length of 24 bits.

```
console(config)#ip address 131.108.1.27 255.255.255.0

console(config)#ip address 131.108.1.27 /24
```

ip address dhcp

Use the **ip address dhcp** command in Global Configuration mode to acquire an IP address for management interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure any acquired address, use the **no** form of this command.

Syntax

ip address {dhcp|bootp|none}

- **dhcp**--Sets protocol to dhcp
- **bootp**--Sets protocol to bootp
- **none**--No protocol is set

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The **ip address dhcp** command allows the switch to dynamically obtain an IP address by using the DHCP protocol.

Example

The following example acquires an IP address for the switch management interface from DHCP.

```
console(config)#ip address dhcp
```

ip address vlan

Use the **ip address vlan** command in Global Configuration mode to set the management VLAN.

Syntax

ip address vlan *vlanid*

no ip address vlan

- *vlanid*—vlan identification. (Range 1-4093)

Default Configuration

The default configuration value is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets VLAN 5 as management VLAN.

```
console(config)#ip address vlan 5
```

ip default-gateway

Use the **ip default-gateway** command in Global Configuration mode to define a default gateway (router).

Syntax

ip default-gateway *ip-address*

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

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

IP address protocol should be set to "none" before setting the gateway.

Example

The following example defines ip default-gateway as `10.240.4.1`.

```
console(config)#ip default-gateway 10.240.4.1
```

ip domain-lookup

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

Syntax

ip domain-lookup

no ip domain-lookup

Default Configuration

The DNS is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

```
console(config)#ip domain-lookup
```

ip domain-name

Use the **ip domain-name** command in Global Configuration mode to define a default domain name used to complete unqualified host names. To delete the default domain name, use the **no** form of this command.

Syntax

ip domain-name *name*

no ip domain-name

- *name*—Default domain name used to complete an unqualified host name. Do not include the initial period that separates the unqualified host name from the domain name (Range: 1-255 characters).

Default Configuration

This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
This command has no user guidelines.

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

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

ip helper-address

Use the **ip helper-address** command in Global Configuration mode to have the device forward User Datagram Protocol (UDP) broadcasts received on an interface. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

Syntax
ip helper-address {*intf-address* | **all**} *ip-address* [*udp-port-list*]

no helper-address {*intf-address* | **all**} *ip-address*

- *intf-address*—IP address of a routing interface. (Range: Any valid IP address)
- **all**—Indicates that this UDP port to address mapping should be used for all IPv4 routing interfaces. The exception is if a particular routing interface has its own mapping, then that mapping takes precedence.
- *ip-address*—Destination broadcast or host address to be used when forwarding UDP broadcasts. You can specify 0.0.0.0 to indicate not to forward the UDP packet to any host. (Range: Any valid IP address)
- *udp-port-list*—The broadcast packet destination UDP port number to forward. If not specified, packets for the default services are forwarded to the helper address. (Range: 0-65535, comma delimited, e.g. 80,100)

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
The **ip helper-address** command forwards specific UDP broadcast from one interface to another. You can define many helper addresses but the total number of address-port pairs is limited to 128 UDP ports for the whole device.

The setting of helper address for specific interface has precedence over a setting of helper address for all the interfaces. You can't enable forwarding of BOOTP/DHCP (ports 67,68) with this command. If you want to relay BOOTP/DHCP packets use the DHCP relay commands.

The **ip helper-address** command specifies a UDP port number for 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)

Example

```
console(config)#ip helper-address 131.108.1.27 10.1.1.1 80,100-
120,201
```

ip host

Use the **ip host** command in Global Configuration mode to define static host name-to-address mapping in the host cache. To delete the name-to-address mapping, use the **no** form of this command.

Syntax

ip host *name address*

no ip host *name*

- *name*—Host name.
- *address*—IP address of the host.

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

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

ip name-server

Use the **ip name-server** command in Global Configuration mode to define available name servers. To delete a name server, use the **no** form of this command.

Syntax

ip name-server *server-address1* [*server-address2* … *server-address8*]

no ip name-server [*server-address1* … *server-address8*]

- *server-address*—Valid IP addresses of the name server. (Range: 1 - 255 characters)

Default Configuration

No name server IP addresses are specified.

Command Mode

Global Configuration mode

User Guidelines

Server preference is determined by entry order.

Up to eight servers can be defined in one command or by using multiple commands.

Example

The following example sets the available name server.

```
console(config)#ip name-server 176.16.1.18
```

show arp switch

Use the **show arp switch** command in Privileged EXEC mode to display the entries in the ARP table used by the management interface.

Syntax

show arp switch

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Note that this command only show ARP entries used by the management interface. It is logically separate from the ARP table used by the routing interfaces. See the **show arp** command for details on how to view ARP entries for the routing interfaces.

Example

The following example displays ARP table information.

```
console#show arp switch

MAC Address          IP Address

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

00:0F:B5:34:90:C5    10.240.4.1
```

show hosts

Use the **show hosts** command in User EXEC mode to display the default domain name, a list of name server hosts, and the static and cached list of host names and addresses. The command itself shows hosts [hostname].

- Host name. (Range: 1 - 255 characters)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about IP hosts.

```
console>show hosts

Host name:

Default domain: gm.com, sales.gm.com, usa.sales.gm.com

Name/address lookup is enabled

Name servers (Preference order): 176.16.1.18 176.16.1.19
```

```
Configured host name-to-address mapping:
Host                            Addresses
-------------------------       ----------------------------
accounting.gm.com               176.16.8.8
Cache:              TTL (Hours)
Host                Total       Elapsed      Type          Addresses
----------------    -----       -------      -------       ---------
----
www.stanford.edu    72          3            IP
171.64.14.203
```

show ip helper-address

Use the **show ip helper-address** command in Privileged EXEC mode to display IP helper addresses configuration.

Syntax

show ip helper-address [*intf-address*]

- *intf-address*—IP address of a routing interface. (Range: Any valid IP address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#show ip helper-address
Interface         Helper Address  Udp port
---------------   --------------- ------------------------
10.1.1.1          1.1.1.1         6
All               1.1.1.1         1,2,3,4,5,6,7,8,9,10,11,
                                  12,13,14,15,16
```

show ip interface management

Use the **show ip interface management** command in User EXEC mode to display the management interface configuration.

Syntax

show ip interface management

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the management interface configuration.

```
console>show ip interface management

IP Address..................................... 10.240.4.125

Subnet Mask.................................... 255.255.255.0

Default Gateway................................ 10.240.4.1

Burned In MAC Address.......................... 00:10:18:82:04:35

Network Configuration Protocol Current......... None

Management VLAN ID............................. 1
```

25

802.1x Commands

aaa authentication dot1x

Use the **aaa authentication dot1x** command in Global Configuration mode to create an authentication login list.

Syntax

aaa authentication dot1x default *method1* [*method2*]

no aaa authentication dot1x default

- *method1* [*method2*]— At least one from the following table:

Keyword	Description
radius	Uses the list of all authentication servers for authentication
none	Uses no authentication

Default Configuration

No authentication method is defined.

Command Mode

Global Configuration mode

User Guidelines

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

Example

The following example uses the **aaa authentication dot1x default** command with no authentication.

```
console(config)# aaa authentication dot1x default none
```

dot1x max-req

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

Syntax

dot1x max-req *count*

no dot1x max-req

- *count* — Number of times that the switch sends an EAP-request/identity frame before restarting the authentication process. (Range: 1 - 10)

Default Configuration

The default value for the *count* parameter is 2.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the number of times that the switch sends an EAP-request/identity frame to 6.

```
console(config)# interface ethernet 1/g16

console(config-if-1/g16)# dot1x max-req 6
```

dot1x port-control

Use the **dot1x port-control** command in Interface Configuration mode to enable manual control of the authorization state of the port. To return to the default setting, use the **no** form of this command.

Syntax

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

no dot1x port-control

- **auto —** Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the switch and the client.
- **force-authorized —** 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 authentication of the client.
- **force-unauthorized —** Denies all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Default Configuration

The default configuration is **auto**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended that you disable the spanning tree or enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to go immediately to the forwarding state after successful authentication.

Example

The following example denies all access through the interface.

```
console(config)# interface ethernet 1/g16

console(config-if-1/g16)# dot1x port-control force-unauthorized
```

dot1x re-authenticate

Use the **dot1x re-authenticate** command in Privileged EXEC mode to enable manually initiating a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

dot1x re-authenticate [**ethernet** *interface*]

- *interface* —Specifies a valid interface number. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following command manually initiates a re-authentication of the 802.1x-enabled port.

```
console# dot1x re-authenticate ethernet 1/g16
```

dot1x re-authentication

Use the **dot1x re-authentication** command in Interface Configuration mode to enable periodic re-authentication of the client. To return to the default setting, use the **no** form of this command.

Syntax

dot1x re-authentication

no dot1x re-authentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables periodic re-authentication of the client.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x re-authentication
```

dot1x system-auth-control

Use the **dot1x system-auth-control** command in Global Configuration mode to enable 802.1x globally. To disable 802.1x globally, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

The default for this command is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables 802.1x globally.

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

dot1x timeout quiet-period

Use the **dot1x timeout quiet-period** command in Interface Configuration mode to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

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

Default Configuration

The switch remains in the quiet state for 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, enter a smaller number than the default.

Example

The following example sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange to 3600.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x timeout quiet-period 3600
```

dot1x timeout re-authperiod

Use the **dot1x timeout re-authperiod** command in Interface Configuration mode to set the number of seconds between re-authentication attempts. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

- *seconds* — Number of seconds between re-authentication attempts. (Range: 300 - 4294967295)

Default Configuration

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of seconds between re-authentication attempts to 300.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x timeout re-authperiod 300
```

dot1x timeout server-timeout

Use the **dot1x timeout server-timeout** command in Interface Configuration mode to set the time that the switch waits for a response from the authentication server. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

- *seconds* — Time in seconds that the switch waits for a response from the authentication server. (Range: 1 - 65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The actual timeout is this parameter or the product of the Radius transmission times the Radius timeout, whichever is smaller

Example

The following example sets the time for the retransmission to the authentication server to 3600 seconds.

```
console(config-if-1/g1)# dot1x timeout server-timeout 3600
```

dot1x timeout supp-timeout

Use the **dot1x timeout supp-timeout** command in Interface Configuration mode to set the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

- *seconds* — Time in seconds that the switch should wait for a response to an EAP-request frame from the client before resending the request. (Range: 1 - 65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the time for the retransmission of an EAP-request frame to the client to 3600 seconds.

```
console(config-if-1/g1)# dot1x timeout supp-timeout 3600
```

dot1x timeout tx-period

Use the **dot1x timeout tx-period** command in Interface Configuration mode to set the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

- *seconds* — Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before resending the request. (Range: 1 - 65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following command sets the number of seconds that the switch waits for a response to an EAP-request/identity frame to 3600 seconds.

```
console(config)# interface ethernet 1/g16

console(config-if-1/g16)# dot1x timeout tx-period 3600
```

show dot1x

Use the **show dot1x** command in Privileged EXEC mode to display 802.1x status for the switch or for the specified interface.

Syntax

show dot1x [**ethernet** *interface*]

- *interface* — A valid Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x port g11 status.

```
console#show dot1x ethernet 1/g2

Administrative mode..............disabled

Port       Admin      Oper         Reauth      Reauth  Username
           Mode       Mode         Control     Period
--------   -------- ----------- --------- ------  --------
1/g2       Auto       Authorized   FALSE       3600    n/a

Quiet Period................................... 60
Transmit Period................................ 30
Maximum Requests............................... 2
Supplicant Timeout............................. 30
Server Timeout (secs).......................... 30
Authenticator PAE State........................ Initialize
Backend Authentication State................... Initialize

console#
```

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

Field	Description
Port	The port number.
Admin mode	The port admin mode. Possible values are: **Force-auth**, **Force-unauth**, **Auto**.
Oper mode	The port oper mode of the port. Possible values are: **Authorized**, **Unauthorized** or **Down**.
Reauth Control	Reauthentication control.
Username	The username representing the identity of the Supplicant. This field shows the username when the port control is **auto**. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.
Quiet period	The number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
Max req	The maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process.
Server timeout	Time in seconds the switch waits for a response from the authentication server before resending the request.
State	The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	Counts the number of times the state machine has received a Success message from the Authentication Server.
Authentication fails	Counts the number of times the state machine has received a Failure message from the Authentication Server.

show dot1x statistics

Use the **show dot1x statistics** command in Privileged EXEC mode to display 802.1x statistics for the specified interface.

Syntax

show dot1x statistics ethernet *interface*

- *interface* — Ethernet port name. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x statistics for the specified interface.

```
console#show dot1x statistics ethernet 1/g2


Port..................................... 1/g2
EAPOL Frames Received.................... 0
EAPOL Frames Transmitted................. 0
EAPOL Start Frames Received.............. 0
EAPOL Logoff Frames Received............. 0
Last EAPOL Frame Version................. 0
Last EAPOL Frame Source.................. 0000.0000.0000
EAP Response/Id Frames Received.......... 0
EAP Response Frames Received............. 0
EAP Request/Id Frames Transmitted........ 0
EAP Request Frames Transmitted........... 0
Invalid EAPOL Frames Received............ 0
EAPOL Length Error Frames Received....... 0
```

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

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

show dot1x users

Use the **show dot1x users** command in Privileged EXEC mode to display 802.1x authenticated users for the switch.

Syntax

show dot1x users [**username** *username*]

- *username* — Supplicant username (Range: 1- 160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x users.

```
console#show dot1x users

Port      Username

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

1/g1       Bob

1/g2       John

Switch# show dot1x users username Bob

Port      Username

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

1/g1       Bob
```

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

Field	Description
Username	The username representing the identity of the Supplicant.
Port	The port that the user is using.

802.1 Advanced Features

dot1x auth-not-req

Use the **dot1x auth-not-req** command in Interface Configuration (VLAN) mode to enable unauthorized devices access to that VLAN. To disable access, use the **no** form of this command.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

User is authorized to access the VLAN.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

An access port cannot be a member in an unauthenticated VLAN. The PVID of a trunk port cannot be an unauthenticated VLAN. For a general port, the PVID can be the unauthenticated VLAN (although only tagged packets would be accepted in the unauthorized state.)

Example

The following example enables unauthorized users access to the VLAN.

```
console(config)#interface vlan 3

console(config-vlan3)#dot1x auth-not-req
```

dot1x guest-vlan

Use the **dot1x guest-vlan** command in Interface Configuration mode to define a guest VLAN. To return to the default settings, use the **no** form of this command.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Default Configuration

No Guest VLAN enabled on interface.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the **dot1x guest-vlan enable** command in Interface Configuration mode to enable unauthorized users on an interface access to the guest VLAN. If the guest VLAN is defined and enabled, the port joins the guest VLAN automatically when the port is unauthorized and leaves the guest VLAN when the port becomes authorized. To make sure this function works, ensure that the port is not a member in the guest VLAN **statically**.

Example

The following example shows how to access the Guest VLAN.

```
console(config-if-vlan1)#dot1x guest-vlan
```

dot1x guest-vlan enable

Use the **dot1x guest-vlan enable** command in Interface Configuration mode to enable unauthorized users on the interface an access to the guest VLAN. To disable the access, use the **no** form of this command.

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Configuration

No Guest VLAN is enabled on the interface.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The switch has one global guest VLAN defined by the **dot1x guest-vlan** Interface VLAN configuration command.

Example

The following example displays how to enable unauthorized users.

```
console(config-if-1/g3)#dot1x guest-vlan enable
```

dot1x multiple-hosts

Use the **dot1x multiple-hosts** command in Interface Configuration mode to allow multiple hosts (clients) on an 802.1x-authorized port where the **dot1x port-control** command is set to **auto**. Use the **no** form of this command to disable multiple hosts.

Syntax

dot1x multiple-hosts

no dot1x multiple-hosts

Default Configuration

Multiple hosts is enabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables the attachment of multiple clients to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

To enable port security on a port, ensure that multiple hosts are enabled.

For unauthenticated VLANs, multiple hosts are always enabled.

Example

The following command allows multiple hosts (clients) on an 802.1x-authorized port.

```
console(config-if-1/g1)#dot1x multiple-hosts
```

dot1x single-host-violation

Use the **dot1x single-host-violation** command in Interface Configuration mode to configure the action to be taken when a station whose MAC address is not the supplicant MAC address attempts to access the interface. To return to the default setting, use the **no** form of this command.

Syntax

dot1x single-host-violation {**forward**|**discard**|**discard-shutdown**}[**trap** *seconds*]

no dot1x single-host-violation

- **forward** — Forward frames with source addresses that are not the supplicant address, but do not learn the address.
- **discard** — Discard frames with source addresses that are not the supplicant address.

- **discard-shutdown** — Discard frames with source addresses that are not the supplicant address, and shut down the port.
- **trap** *seconds*— Send SNMP traps and specifies the minimum time in seconds between consecutive traps. (Range: 1- 1000000**)**

Default Configuration

Discard frames with source addresses that are not the supplicant address. No traps.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command is relevant when Multiple Hosts is disabled and the user has been authenticated successfully.

Example

The following example uses forward action to forward frames with source addresses that are not the supplicant address.

```
console(config-if-1/g1)#dot1x single-host-violation forward trap
100
```

show dot1x advanced

Use the **show dot1x advanced** command in Privileged EXEC mode to display 802.1x advanced features for the switch or for the specified interface.

Syntax

show dot1x advanced [**ethernet** *interface*]

- *interface* — Specifies a valid ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x advanced features for the switch.

```
console#show dot1x advanced
Guest VLAN: 3978
Unauthenticated VLANs: 91, 92

Port        Multiple    Guest
            Hosts       VLAN
---------   ---------   ------
1/g1        Disabled    Enabled
1/g2        Enabled     Disabled

console# show dot1x advanced ethernet 1/g1
Port       Multiple   Guest
           Hosts      VLAN
---------  ---------  ------
1/g1       Disabled   Enabled

Single host parameters
Violation action: Discard
Trap: Enabled
Trap frequency: 100
Status: Single-host locked
Violations since last trap: 9
```

26

Configuration and Image File Commands

boot system

Use the **boot system** command in Privileged EXEC mode to specify the system image that the device loads at startup.

Syntax

boot system [image1 | image2]

- **image1 | image2**— Image file.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

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

Example

The following example loads system image **image1** for the next device startup.

```
console# boot system image1
```

clear config

Use the **clear config** command in Privileged EXEC mode to restore the switch to the default configuration.

Syntax

clear config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example restores the switch to its default configuration.

```
console#clear config
```

copy

Use the **copy** command in Privileged EXEC mode to copy files from a source to a destination.

Syntax

copy *source-url destination-url*

- *source-url* —The location URL or reserved keyword of the source file being copied. (Range: 1-160 characters.)
- *destination-url* —The URL or reserved keyword of the destination file. (Range: 1-160 characters.)

The following table lists and describes reserved keywords

Reserved Keyword	Description
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.
startup-log	Represents the startup syslog file. This can only be the source of a copy operation.
operational-log	Represents the operational syslog file. This can only be the source of a copy operation.
script *scriptname*	Represents a CLI script file.
image	Represents the software image file. When "image" is the target of a copy command, it refers to the backup image. When "image" is the source of a copy command, it refers to the active image. If this is destination, the file will be distributed to all units in the stack.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:***[[//location]/directory]/filename*. An out-of-band IP address can be specifed as described in the User Guidelines.

Reserved Keyword	Description
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
backup-config	Represents the backup configuration file.
unit	Indicates which unit in the stack is the target of the copy command.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

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

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

Understanding Invalid Combinations of Source and Destination

Some combinations of source and destination are not valid. Specifically, if the following conditions exist, you can not use the **copy** command:

- If the source file and destination file are defined to be the same.
- **xmodem** cannot be a source and destination for the same copy operation. **xmodem** can only be copied to **image**.
- **tftp** cannot be the source and destination for the same copy operation.

The following table contains copy character descriptions.

Copying Image File from a Server to Flash Memory

Use the **copy source-url image** command to copy an image file from a server to flash memory Use the **boot system** command to activate the new image.

Copying a Configuration File from a Server to the Running Configuration

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

Copying a Configuration File from a Server to the Startup Configuration

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

Storing the Running or Startup Configuration on a Server

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

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

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.

Copying to a Unit on the Stack Using unit

The **copy** command can be used to copy an image to another unit. This means that a **copy** command allows the management node to distribute its existing code to other nodes. The command syntax is **copy image unit {all | <1-12>}**

NOTE: The copy command can accept the **unit {all | <1-12>}** only as the destination-url. In this case, only **image** can be the source-url.

NOTE: Note that the **copy image unit all** command does not copy the active image to the backup image on the management unit, just the stack units.

The **copy** command can not:

- Either download code from tftp, for example, to the stack units directly, or
- Copy code from one stack unit to another stack unit.

For copying to all units simultaneously, use the keyword **all**.

Example

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 in flash memory.

```
console#copy tftp://172.16.101.101/pc62xxr1v0.stk image
Mode..................................... TFTP
Set TFTP Server IP....................... 172.16.101.101
TFTP Path................................ ./
TFTP Filename............................ pc62xxr1v0.stk
Data Type................................ Code
```

```
Destination Filename..... image1
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP code transfer starting
```

delete backup-config

Use the **delete backup-config** command in Privileged EXEC mode to delete the backup-config file.

Syntax

delete backup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example deletes the backup-config file.

```
console#delete backup-config
Delete backup-config (Y/N)?y
```

delete backup-image

Use the **delete backup-image** command in Privileged EXEC mode to delete a file from a flash memory device.

Syntax

delete backup-image

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Note that the active image cannot be deleted.

Example

The following example deletes test file in Flash memory.

```
console#delete backup-image
Delete: image2 (y/n)?
```

delete startup-config

Use the **delete startup-config** command in Privileged EXEC mode to delete the startup-config file.

Syntax

delete startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the startup-config file is not present when system reboots, it reboots with default settings.

Example

The following example deletes the startup-config file.

```
console# delete startup-config
Delete startup-config (y/n)?
```

filedescr

Use the **filedescr** command in Privileged EXEC mode to add a description to a file. Use the **no** version of this command to remove the description from the filename.

Syntax

filedescr {image 1|image2} *description*

no filedescr {image 1|image2}

- **image1|image2**— Image file.
- *description*—Block of descriptive text. (Range: 0-128 characters)

Default Configuration

No description is attached to the file.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example attaches a file description to image2.

```
console#filedescr image2 "backedup on 03-22-05"
```

ftpdownload

Use the **ftpdownload** command to update the backup image on the switch. Users can use the **boot system image1/image2** command to appropriately load the image on next reload.

This command can be executed by a script. Password protection is not provided, and the password is displayed on the CLI console as it is typed by the user or given in the script.

Syntax Description

ftpdownload *ipaddress/path* **image user** *user name* **password** *password*

- *Ipaddress/path*—IP address of FTP server followed by the destination directory path from which the image file is to be downloaded. (Range: Valid IP address and directory from which the image file is to be downloaded)
- *image*—Specifies the backup image on flash. (Range: None)
- *Username*—User name on the FTP server. (Range: Valid user name)
- *Password*—Password for the respective user on the FTP server. (Range: Valid password)

Command Mode

Privileged EXEC

Default Configuration

This command has no default configuration

User Guidelines

No specific guidelines.

Example

```
console#ftpdownload 10.240.3.108/dell/image1 image user randall
password DellRandall


Mode..................................... FTP
Set FTP Server IP........................ 10.240.3.108
FTP Path................................. ./dell
FTP Filename............................. image1
Data Type................................ Code
Destination Filename..................... image

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

FTP code transfer starting

.....

File transfer complete!

console#
```

script apply

Use the **script apply** command in Privileged EXEC mode to apply the commands in the script to the switch.

Syntax

script apply *scriptname*

- *scriptname*—Name of the script file to apply. (Range 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example applies the *config.scr* script to the switch.

```
console#script apply config.scr
```

script delete

Use the **script delete** command in Privileged EXEC mode to delete a specified script.

Syntax
script delete {*scriptname* | **all}**

- *scriptname*—Script name of the file being deleted. (Range 1-31 characters)

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example deletes all scripts from the switch.

```
console#script delete all
```

script list

Use the **script list** command in Privileged EXEC mode to list all scripts present on the switch as well as the remaining available space.

Syntax
script list

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example displays all scripts present on the switch.

```
console#script list
Configuration Script Name Size(Bytes)
-------------------------------- -----------
0 configuration script(s) found.
2048 Kbytes free.
```

script show

Use the **script show** command in Privileged EXEC mode to display the contents of a script file.

Syntax
script show *scriptname*

- *scriptname*—Name of the script file to be displayed. (Range: 1-31 characters)

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example displays the contents of the script file *config.scr.*

```
console#script show config.scr
interface ethernet 1/g1
ip address 176.242.100.100 255.255.255.0
exit
```

script validate

Use the **script validate** command in Privileged EXEC mode to validate a script file by parsing each line in the script file.The validate option is intended for use as a tool in script development. Validation identifies potential problems though it may not identify all problems with a given script.

Syntax

script validate *scriptname*

- *scriptname*—Name of the script file being validated. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example validates the contents of the script file *config.scr.*

```
console#script validate config.scr
```

show backup-config

Use the **show backup-config** command in Privileged EXEC mode to display the contents of the backup configuration file.

Syntax

show backup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows backup-config data.

```
console#show backup-config
software version 1.1
hostname device
interface ethernet 1/g1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000
exit
interface ethernet 1/g2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
exit
```

show bootvar

Use the **show bootvar** command in User EXEC mode to display the active system image file that the device loads at startup.

Syntax

show bootvar [*unit*]

- *unit*—-Unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console>show bootvar
```

```
Image Descriptions
 image1 : default image
 image2 :

 Images currently available on Flash

--------------------------------------------------------------------
--
 unit      image1      image2     current-active        next-active
--------------------------------------------------------------------
--

    1    0.31.0.0    0.31.0.0             image2              image2
```

show dir

Use the **show dir** command to list all the files available on the flash file system (TrueFlashFileSystem). The user can view the file names, the size of each file, and the date of the last modification.

Syntax Description

show dir

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
console#show dir
File name          Size (in bytes)
```

```
---------           ---------------
image1              6351288
image2              6363424
fastpath.cfg        321894
```

show running-config

Use the **show running-config** command in Privileged EXEC mode to display the contents of the currently running configuration file.

Syntax

show running-config [*all* | *scriptname*]

- *all*-—To display or capture the commands with settings and configuration that are equal to the default value, include the *all* option.
- *scriptname*-—The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *scriptname* is provided with a file name extension of ".scr", the output is redirected to a script file.

NOTE: If you issue the **show running-config** command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#show running-config
software version 1.1
hostname device
interface ethernet 1/g1
    ip address 176.242.100.100 255.255.255.0
```

```
    duplex full
    speed 1000
exit
interface ethernet 1/g2
    ip address 176.243.100.100 255.255.255.0
    duplex full
    speed 1000
exit
```

show startup-config

Use the **show startup-config** command in Privileged EXEC mode to display the startup configuration file contents.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

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

```
console#show startup-config
software version 1.1
hostname device
interface ethernet 1/g1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000
```

```
exit
interface ethernet 1/g2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
exit
```

update bootcode

Use the **update bootcode** command in Privileged EXEC mode to update the bootcode on one or more switches. For each switch, the bootcode is extracted from the active image and programmed to flash.

Syntax

update bootcode [*unit*]

- *unit* —Unit number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If *unit* is not specified, all units are updated.

Example

The following example updates the bootcode on unit 2.

```
console#update bootcode 2
```

27

QoS Commands

assign-queue

Use the **assign-queue** command in Policy-Class-Map Configuration mode to modify the queue ID to which the associated traffic stream is assigned.

Syntax

assign-queue <*queueid*>

- *queueid*—Specifies a valid queue ID. (Range: integer from 0–6.)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to change the queue ID to 4 for the associated traffic stream.

```
console(config-policy-classmap)#assign-queue 4
```

class

Use the **class** command in Policy-Map Class Configuration mode to create an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.

Syntax

class *classname*

no class

- *classname*—Specifies the name of an existing DiffServ class. (Range: 1 - 31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command causes the specified policy to create a reference to the class definition. The command mode is changed to Policy-Class-Map Configuration when this command is executed successfully.

Example

The following example shows how to specify the DiffServ class name of "DELL."

```
console(config)#policy-map DELL1
console(config-policy-classmap)#class DELL
```

class-map

Use the **class-map** command in Global Configuration mode to define a new DiffServ class of type *match-all*. To delete the existing class, use the **no** form of this command.

Syntax

class-map [match-all]*classmapname*

no class-map *classmapname*

- match-all—Use this option to create a new class-map. Usage of this option is mandatory if a new class is created.
- *classmapname*—Specifies the name of a DiffServ class consisting of a character string that can be up to 31 characters long. (Range: 1 - 31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The CLI mode is changed to Class-Map Configuration when this command is executed successfully.

Example

The following example creates a class-map named "DELL" which requires all ACE's to be matched.

```
console(config)#class-map DELL

console(config-cmap)#
```

class-map rename

Use the **class-map rename** command in Global Configuration mode to change the name of a DiffServ class.

Syntax

class-map rename <*classname*> <*newclassname*>

- *classname*—The name of an existing DiffServ class. (Range: 1 - 31 characters)
- *newclassname*—A case-sensitive alphanumeric string. (Range: 1 - 31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to change the name of a DiffServ class from "DELL" to "DELL1."

```
console(config)#class-map rename DELL DELL1

console(config)#
```

classofservice dot1p-mapping

Use the **classofservice dot1p-mapping** command in Global Configuration mode to map an 802.1p priority to an internal traffic class. In Interface Configuration mode, the mapping is applied only to packets received on that interface. Use the **no** form of the command to remove mapping between an 802.1p priority and an internal traffic class.

Syntax

classofservice dot1p-mapping *802.1ppriority trafficclass*

no classofservice dot1p-mapping

- *802.1ppriority*—Specifies the user priority mapped to the specified traffic class for this switch. (Range: 0 - 7)
- *trafficclass*—Specifies the traffic class for this switch. (Range: 0 - 6)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

None

Example

The following example configures mapping for user priority 1 and traffic class 2.

```
console(config)#classofservice dot1p-mapping 1 2
```

classofservice ip-dscp-mapping

Use the **classofservice ip-dscp-mapping** command in Global Configuration mode to map an IP DSCP value to an internal traffic class.

Syntax

classofservice ip-dscp-mapping *ipdscp trafficclass*

- *ipdscp*—Specifies the IP DSCP value to which you map the specified traffic class. (Range: 0 - 63)
- *trafficclass*—Specifies the traffic class for this value mapping. (Range: 0 - 6)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays mapping for IP DSCP 1 and traffic class 2.

```
console(config)#classofservice ip-dscp-mapping 1 2
```

classofservice trust

Use the **classofservice trust** command in either Global Configuration mode or Interface Configuration mode to set the class of service trust mode of an interface. To set the interface mode to untrusted, use the **no** form of this command.

Syntax

classofservice trust {dot1p|ip-precedence|ip-dscp}

no classofservice trust

- **dot1p**—Specifies that the mode be set to trust dot1p (802.1p) packet markings.
- **ip-precedence**—Specifies that the mode be set to trust IP Precedence packet markings.
- **ip-dscp**—Specifies that the mode be set to trust IP DSCP packet markings.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays how you set the class of service trust mode of an interface to trust dot1p (802.1p) packet markings when in Global Configuration mode.

```
console(config)#classofservice trust dot1p
```

The following example displays how you set the class of service trust mode of an interface to trust IP Precedence packet mark

```
console(config)#classofservice trust ip-precedence
```

conform-color

Use the **conform-color** command in Policy-Class-Map Configuration mode to specify second-level matching for traffic flow, the only possible actions are drop, set-cos-transmit, setdscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the policy command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command.

Syntax

conform-color

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to specify the **conform-color** command.

```
console(config-policy-classmap)#conform-color test_class
(test_class is <class-map-name>
```

cos-queue min-bandwidth

Use the **cos-queue min-bandwidth** command in either Global Configuration mode or Interface Configuration mode to specify the minimum transmission bandwidth for each interface queue. To restore the default for each queue's minimum bandwidth value, use the **no** form of this command.

Syntax

cos-queue min-bandwidth *bw-0 bw-1 … bw-n*

no cos-queue min-bandwidth

- *bw-0*—Specifies the minimum transmission bandwidth for an interface. You can specify as many bandwidths as there are interfaces (bw-0 through bw-n). (Range: 0 - 100 in increments of 5)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The maximum number of queues supported per interface is seven.

Example

The following example displays how to specify the minimum transmission bandwidth for seven interfaces.

```
console(config)#cos-queue min-bandwidth  0 0 5 5 10 10 10
```

cos-queue strict

Use the **cos-queue strict** command in either Global Configuration mode or Interface Configuration mode to activate the strict priority scheduler mode for each specified queue. To restore the default weighted scheduler mode for each specified queue, use the **no** form of this command.

Syntax

cos-queue strict {*queue-id-1*} [{*queue-id-2*} … {*queue-id-n*}]

no cos-queue strict {*queue-id-1*} [{*queue-id-2*} … {*queue-id-n*}]

- **queue-id-1**—Specifies the queue ID for which you are activating the strict priority scheduler. You can specify a queue ID for as many queues as you have (queue-id 1 through queue-id-n). (Range: 0 - 6)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to activate the strict priority scheduler mode for two queues.

```
console(config)#cos-queue strict 1 2
```

The following example displays how to activate the strict priority scheduler mode for three queues.

```
console(config)#cos-queue strict 1 2 4
```

diffserv

Use the **diffserv** command in Global Configuration mode to set the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated. To set the DiffServ operational mode to inactive, use the **no** form of this command.

Syntax

diffserv

no diffserv

Default Configuration

This command default is **enabled**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to set the DiffServ operational mode to active.

```
console(Config)#diffserv
```

drop

Use the **drop** command in Policy-Class-Map Configuration mode to specify that all packets for the associated traffic stream are to be dropped at ingress.

Syntax

drop

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to specify that matching packets are to be dropped at ingress.

```
console(config-policy-classmap)#drop
```

mark cos

Use the **mark cos** command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.

Syntax

mark cos *cos-value*

- *cos-value*—Specifies the CoS value as an integer. (Range: 0 - 7)

Default Configuration

The default value for this command is 1.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to mark all packets with a CoS value.

```
console(config-policy-classmap)#mark cos 7
```

mark ip-dscp

Use the **mark ip-dscp** command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified IP DSCP value.

Syntax

mark ip-dscp *dscpval*

- *dscpval*—Specifies the DSCP value as an integer or keyword value. (Integer Range: 0 - 63) (Keyword values: *af11*, *af12*, *af13*, *af21*, *af22*, *af23*, *af31*, *af32*, *af33*, *af41*, *af42*, *af43*, *be*, *cs0*, *cs1*, *cs2*, *cs3*, *cs4*, *cs5*, *cs6*, *cs7*, *ef*)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to mark all packets with an IP DSCP value of "cs4."

```
console(config-policy-classmap)#mark ip-dscp cs4
```

mark ip-precedence

Use the **mark ip-precedence** command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified IP precedence value.

Syntax

mark ip-precedence *prec-value*

- *prec-value*—Specifies the IP precedence value as an integer. (Range: 0 - 7)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines.

This command has no user guidelines.

Example

The following example displays

```
console(config(#policy-map p1 in
console(config-policy-map)#class c1
console(config-policy-classmap)#mark ip-precedence 2
console(config-policy-classmap)#
```

match class-map

Use the **match class-map** command to add to the specified class definition the set of match conditions defined for another class. Use the **no** form of this command to remove from the specified class definition the set of match conditions defined for another class.

Syntax

match class-map *refclassname*

no match class-map *refclassname*

- *refclassname*—The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

- The parameters *refclassname* and *class-map-name* can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the *refclassname* class while the class is still referenced by any *class-map-name* fails.
- The combined match criteria of *class-map-name* and *refclassname* must be an allowed combination based on the class type.
- Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

Example

The following example adds match conditions defined for the Dell class to the class currently being configured.

```
console(config-classmap)#match class-map Dell
```

The following example deletes the match conditions defined for the Dell class from the class currently being configured.

```
console(config-classmap)#no match class-map Dell
```

match cos

Use the **match cos** command in Class-Map Configuration mode to add to the specified class definition a match condition for the class of service value (the only tag in a single-tagged packet or the first or outer 802.1Q tag of a double-VLAN tagged packet).

Syntax

match cos

- cos-value—Specifies the CoS value as an integer (Range: 0 - 7)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition to the specified class.

```
console(config-classmap)#match cos 1
```

match destination-address mac

Use the **match destination-address mac** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination MAC address of a packet.

Syntax

match destination-address mac *macaddr macmask*

- *macaddr*—Specifies any valid layer 2 MAC address formatted as six two-digit hexadecimal numbers separated by colons.
- *macmask*—Specifies a valid layer 2 MAC address bit mask formatted as six two-digit hexadecimal numbers separated by colons. This address bit mask does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition for the specified MAC address and bit mask.

```
console(config-classmap)#match destination-address mac
AA:ED:DB:21:11:06  FF:FF:FF:EF:EE:EE
```

match dstip

Use the **match dstip** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination IP address of a packet.

Syntax

match dstip *ipaddr ipmask*

- *ipaddr*—Specifies a valid IP address.
- *ipmask*—Specifies a valid IP address bit mask. Note that even though this parameter is similar to a standard subnet mask, it does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition using the specified IP address and bit mask.

```
console(config-classmap)#match dstip 10.240.1.1 10.240.0.0
```

match dstl4port

Use the **match dstl4port** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or a numeric notation.

Syntax

match dstl4port {*portkey*|*port-number*}

- *portkey*—Specifies one of the supported port name keywords. A match condition is specified by one layer 4 port number. The currently supported values are: domain, echo, ftp, ftpdata, http, smtp,snmp, telnet, tftp, and www.
- *port-number*—Specifies a layer 4 port number (Range: 0–65535).

Default Configuration

This command has no default configuration.

Command Mode

Class-Map configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition based on the destination layer 4 port of a packet using the "echo" port name keyword.

```
console(config-classmap)#match dstl4port echo
```

match ethertype

Use the **match ethertype** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the ethertype.

Syntax

match ethertype {**keyword**|<*0x0600-0xffff*> }

- **keyword**—Specifies either a valid keyword or a valid hexadecimal number. The supported keywords are **appletalk**, **arp, ibmsna**, **ipv4, ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, **rarp**. (Range: 0x0600 - 0xFFFF)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add a match condition based on ethertype.

```
console(config-classmap)#match ethertype arp
```

match ip dscp

Use the **match ip dscp** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet. This field is defined as the high-order six bits of the Service Type octet in the IP header. The low-order two bits are not checked.

Syntax

match ip dscp *dscpval*

- *dscpval*—Specifies an integer value or a keyword value for the DSCP field. (Integer Range: 0 - 63) (Keyword Values: *af11*, *af12*, *af13*, *af21*, *af22*, *af23*, *af31*, *af32*, *af33*, *af41*, *af42*, *af43*, *be*, *cs0*, *cs1*, *cs2*, *cs3*, *cs4*, *cs5*, *cs6*, *cs7*, *ef*)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

The **ip dscp**, **ip precedence**, and **ip tos** match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

To specify a match on all DSCP values, use the **match ip tos** *tosbits tosmask* command with tosbits set to "0" (zero) and tosmask set to hex "03."

Example

The following example displays how to add a match condition based on the DSCP field.

```
console(config-classmap)# match ip dscp 3
```

match ip precedence

Use the **match ip precedence** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP precedence field.

Syntax

match ip precedence *precedence*

- *precedence*—Specifies the precedence field in a packet. This field is the high-order three bits of the Service Type octet in the IP header. (Integer Range: 0 - 7)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

The **ip dscp**, **ip precedence**, and **ip tos** match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

To specify a match on all precedence values, use the **match ip tos** *tosbits tosmask* command with tosbits set to "0" (zero) and tosmask set to hex "1F."

Example

The following example displays adding a match condition based on the value of the IP precedence field.

```
console(config-classmap)#match ip precedence 1
```

match ip tos

Use the **match ip tos** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP TOS field in a packet. This field is defined as all eight bits of the Service Type octet in the IP header.

Syntax

match ip tos *tosbits tosmask*

- *tosbits*—Specifies a two-digit hexadecimal number. (Range: 00 - ff)
- *tosmask*—Specifies the bit positions in the tosbits parameter that are used for comparison against the IP TOS field in a packet. This value of this parameter is expressed as a two-digit hexadecimal number. (Range: 00 - ff)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

The **ip dscp**, **ip precedence**, and **ip tos** match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

This specification is the *free form* version of the IP DSCP/Precedence/TOS match specification in that you have complete control of specifying which bits of the IP Service Type field are checked.

Example

The following example displays adding a match condition based on the value of the IP TOS field in a packet.

```
console(config-classmap)#match ip tos AA EF
```

match protocol

Use the **match protocol** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

Syntax

match protocol {*protocol-name*|*protocol-number*}

- *protocol-name*—Specifies one of the supported protocol name keywords. The supported values are *icmp*, *igmp*, *ip*, *tcp*, and *udp*.
- *protocol-number*—Specifies the standard value assigned by IANA. (Range 0 - 255)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition based on the "ip" protocol name keyword.

```
console(config-classmap)#match protocol ip
```

match source-address mac

Use the **match source-address mac** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source MAC address of the packet.

Syntax

match source-address mac *address macmask*

- *macaddr*—Specifies any valid layer 2 MAC address formatted as six two-digit hexadecimal numbers separated by colons.
- *macmask*—Specifies a layer 2 MAC address bit mask formatted as six two-digit hexadecimal numbers separated by colons. This bit mask does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example adds to the specified class definition a match condition based on the source MAC address of the packet.

```
console(config-classmap)# match source-address mac
10:10:10:10:10:10 11:11:11:11:11:11
```

match srcip

Use the **match srcip** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source IP address of a packet.

Syntax

match srcip *ipaddr ipmask*

- *ipaddr*—Specifies a valid IP address.

- *ipmask*—Specifies a valid IP address bit mask. Note that although this IP address bit mask is similar to a subnet mask, it does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition for the specified IP address and address bit mask.

```
console(config-classmap)#match srcip 10.240.1.1 10.240.0.0
```

match srcl4port

Use the **match srcl4port** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or a numeric notation.

Syntax

match srcl4port {*portkey*|*port-number*}

- *portkey*—Specifies one of the supported port name keywords. A match condition is specified by one layer 4 port number. The currently supported values are: domain, echo, ftp, ftpdata, http, smtp,snmp, telnet, tftp, and www.
- *port-number*—Specifies a layer 4 port number (Range: 0–65535).

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

None

Example

The following example displays how to add a match condition using the "snmp" port name keyword.

```
console(config-classmap)#match srcl4port snmp
```

match vlan

Use the **match vlan** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field. This field is the only tag in a single tagged packet or the first or outer tag of a double VLAN packet.

Syntax

match vlan <*vlan-id*>

- <*vlan-id*>—Specifies a VLAN ID as an integer. (Range: 0 - 4095)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition for the VLAN ID "2."

```
console(config-classmap)#match vlan 2
```

mirror

Use the **mirror** command in Policy-Class-Map Configuration mode to mirror all the data that matches the class defined to the destination port specified.

Syntax

mirror *interface*

- *interface*—Specifies the Ethernet port to which data needs to be copied.

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

The port identified in this command is identical to the destination port of the **monitor** command.

Example

The following example displays how to copy all the data to ethernet port 1/g5.

```
console(config-policy-classmap)#mirror 1/g5
```

police-simple

Use the **police-simple** command in Policy-Class-Map Configuration mode to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and nonconform.

Syntax

police-simple {<*datarate*> <*burstsize*> **conform-action** {**drop** | **set-cos-transmit** <*cos*> | **set-prectransmit** <*cos*> | **set-dscp-transmit** <*dscpval*> | **transmit**} [**violateaction** {**drop** | **set-cos-transmit** <*cos*> | **set-prec-transmit** <*cos*> | **set-dscp-transmit** <*dscpval*> | **transmit**}]}

- *datarate*—Data rate in kilobits per second (kbps). (Range: 1–4294967295)
- *burstsize*—Burst size in Kbps (Range: 1–128)
- **conform action**—Indicates what happens when the packet is conforming to the policing rule: it could be dropped, it could have its COS modified, it could have its IP precedence modified, or it could have its DSCP modified. The same actions are available for packets that do not conform to the policing rule.
- *cos*—Class of Service value. (Range: 0 - 7)
- dscpval—DSCP value. (Range: 0 - 63 or a keyword from this list, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **ef**)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

Only one style of police command (simple) is allowed for a given class instance in a particular policy.

Example

The following example shows how to establish the traffic policing style for the specified class.

```
console(config-policy-classmap)#police-simple 33 34 conform-action
transmit violate-action transmit
```

policy-map

Use the **policy-map** command in Global Configuration mode to establish a new DiffServ policy. To remove the policy, use the **no** form of this command.

Syntax

policy-map *policyname* [**in**]

no policy-map *policyname*

- *policyname*—Specifies the DiffServ policy name as a unique case-sensitive alphanumeric string of characters. (Range: 1 - 31 alphanumeric characters.)
- **in**—Inbound direction. Must be specified for new DiffServ policies. Not specified for existing DiffServ policies. A new policy can be specified with "in" only. An existing policy can be entered without "in" only.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The CLI mode is changed to Policy-Class-Map Configuration when this command is successfully executed.

The policy type dictates which of the individual policy attribute commands are valid within the policy definition.

Example

The following example shows how to establish a new DiffServ policy named "DELL."

```
console(config)#policy-map DELL

console(config-policy-classmap)#
```

redirect

Use the **redirect** command in Policy-Class-Map Configuration mode to specify that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Syntax

redirect *interface*

- *interface*—Specifies any valid interface. Interface is Ethernet port or port-channel (Range: lag1–lag18)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to redirect incoming packets to port 1/g1.

```
console(config-policy-classmap)#redirect 1/g1
```

service-policy

Use the **service-policy** command in either Global Configuration mode (for all system interfaces) or Interface Configuration mode (for a specific interface) to attach a policy to an interface. To return to the system default, use the **no** form of this command.

Syntax

service-policy in *policymapname*

no service-policy in *policymapname*

- *policymapname*—Specifies the DiffServ policy name as a unique case-sensitive alphanumeric string. (Range: 1 - 31 alphanumeric characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode (for all system interfaces)

Interface Configuration (Ethernet, Port-channel) mode (for a specific interface)

User Guidelines

This command effectively enables DiffServ on an interface. No separate interface administrative mode command for DiffServ is available.

Ensure that no attributes within the policy definition exceed the capabilities of the interface. When a policy is attached to an interface successfully, any attempt to change the policy definition, such that it would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Example

The following example shows how to attach a service policy named "DELL" to all interfaces.

```
console(config)#service-policy DELL
```

show class-map

Use the **show class-map** command in Privileged EXEC mode to display all configuration information for the specified class.

Syntax

show class-map [*classname*]

- *classname*—Specifies the valid name of an existing DiffServ class. (Range: 1 - 31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all the configuration information for the class named "Dell".

```
console#show class-map DELL

Class Name..................................... DELL
Class Type..................................... All

      Match Criteria                          Values
-------------------------- ------------------------------------
```

show classofservice dot1p-mapping

Use the **show classofservice dot1p-mapping** command in Privileged EXEC mode to display the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.

Syntax

show classofservice dot1p-mapping [<*unit*>/<*port-type*><*port*>|**port-channel** *port-channel number*]

- <*unit*>/<*port-type*><*port*>—Specifies a valid unit/port combination.
  <*unit*>—Physical switch identifier within the stack. Values are *1-12*.
  <*port-type*>— Values are **g** for gigabit Ethernet port, or **xg** for 10 gigabit Ethernet port.
  <*port*>—port number. Values are *1-24* or *1-48* in the case of port_type g, and 1-4 for port_type xg.
  Example: xg2 is the 10 gigabit Ethernet port 2.
- *port-channel number*—Specifies a valid port-channel number. Range is 1-8.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the interface is specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Example

The following example displays the dot1p traffic class mapping and user priorities.

```
console#show classofservice dot1p-mapping

 User Priority    Traffic Class
 -------------    ---------------
       0               1
       1               1
       2               6
       3               4
       4               3
       5               4
       6               5
       7               6
```

The following table lists the parameters in the example and gives a description of each.

Parameter	Description
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

Use the **show classofservice ip-dscp-mapping** command in Privileged EXEC mode to display the current IP DSCP mapping to internal traffic classes for a specific interface.

Syntax

show classofservice ip-dscp-mapping

- Command is supported only globally.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Example

```
console#show classofservice ip-dscp-mapping


    IP DSCP       Traffic Class
 -------------    -------------
   0(be/cs0)           1
   1                   1
   2                   1
   3                   1
   4                   1
   5                   1
   6                   1
```

```
   7                    1
   8(cs1)               0
   9                    0
   10(af11)             0
   11                   0
   12(af12)             0
   13                   0
   14(af13)             0
   15                   0
   16(cs2)              0
   17                   0
   18(af21)             0
   19                   0
--More-- or (q)uit
   20(af22)             0
   21                   0
   22(af23)             0
   23                   0
   24(cs3)              1
   25                   1
   26(af31)             1
   27                   1
   28(af32)             1
   29                   1
   30(af33)             1
   31                   1
   32(cs4)              2
   33                   2
   34(af41)             2
```

```
    35                  2
    36(af42)            2
    37                  2
    38(af43)            2
    39                  2
    40(cs5)             2
    41                  2
    42                  2
--More-- or (q)uit
    43                  2
    44                  2
    45                  2
    46(ef)              2
    47                  2
    48(cs6)             3
    49                  3
    50                  3
    51                  3
    52                  3
    53                  3
    54                  3
    55                  3
    56(cs7)             3
    57                  3
    58                  3
    59                  3
    60                  3
    61                  3
    62                  3
```

```
   63                    3


console#
```

show classofservice trust

Use the **show classofservice trust** command in Privileged EXEC mode to display the current trust mode setting for a specific interface.

Syntax

show classofservice trust [<*unit*>/<*port-type*><*port*>|**port-channel** *port-channel number*]

- <*unit*>/<*port-type*><*port*>—Specifies a valid unit/port combination:
  <*unit*>—Physical switch identifier within the stack. Values are *1-12*.
  <*port-type*>— Values are **g** for gigabit Ethernet port, or **xg** for 10 gigabit Ethernet port.
  <*port*>—port number. Values are *1-24* or *1-48* in the case of port_type g, and 1-4 for port_type xg.
  Example: xg2 is the 10 gigabit Ethernet port 2.
- *port-channel number*—Specifies a valid port-channel number. Range is 1-8.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the interface is specified, the port trust mode of the interface is displayed. If omitted, the port trust mode for global configuration is shown.

Example

The following example displays the current trust mode settings for the specified port.

```
console#show classofservice trust 1/g2
Class of Service Trust Mode: Dot1P
```

show diffserv

Use the **show diffserv** command in Privileged EXEC mode to display the DiffServ general information, which includes the current administrative mode setting as well as the current and maximum number of DiffServ components.

Syntax

show diffserv

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DiffServ information.

```
console#show diffserv

DiffServ Admin mode.............................. Enable
Class Table Size Current/Max..................... 5 / 25
Class Rule Table Size Current/Max................ 6 / 150
Policy Table Size Current/Max.................... 2 / 64
Policy Instance Table Size Current/Max......... 2 / 640
Policy Attribute Table Size Current/Max........ 2 / 1920
Service Table Size Current/Max................. 26 / 214
```

show diffserv service interface ethernet in

Use the **show diffserv service interface ethernet** command in Privileged EXEC mode to display policy service information for the specified interface.

Syntax

show diffserv service interface ethernet *<unit>/<port-type><port>* **in**

- *<unit>/<port-type><port>*—A valid *<unit>/<port-type><port>* in the system.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Example

```
console#show diffserv service interface ethernet 1/g1 in

DiffServ Admin Mode.......................... Enable
Interface.................................... 1/g1
Direction.................................... In
No policy is attached to this interface in this direction.
```

show diffserv service interface port-channel in

Syntax Description

show diffserv service interface port-channel *channel-group* **in**

- *channel-group*: A valid port-channel in the system. (Range: 1–18)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

Not applicable

Example

```
console#show diffserv service interface port-channel 1 in

DiffServ Admin Mode.......................... Enable
Interface.................................... ch1
Direction.................................... In
No policy is attached to this interface in this direction
```

show diffserv service brief

Use the **show diffserv service brief** command in Privileged EXEC mode to display all interfaces in the system to which a DiffServ policy has been attached.

Syntax

show diffserv service brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display all interfaces in the system to which a DiffServ policy has been attached.

```
console# show diffserv service brief
Interface     Direction   OperStatus  Policy Name
------------ ----------- ------------ -------------------
1/g1          in          Down        DELL
```

show interfaces cos-queue

Use the **show interfaces cos-queue** command in Privileged EXEC mode to display the class-of-service queue configuration for the specified interface.

Syntax

show interfaces cos-queue [<*unit*>/<*port-type*><*port*>|**port-channel** *port-channel number*]

- <*unit*>/<*port-type*><*port*>—Specifies a valid unit/port combination:
  <*unit*>—Physical switch identifier within the stack. Values are *1-12*.
  <*port-type*>— Values are **g** for gigabit Ethernet port, or **xg** for 10 gigabit Ethernet port.
  <*port*>—port number. Values are *1-24* or *1-48* in the case of port_type g, and 1-4 for port_type xg.
  Example: xg2 is the 10 gigabit Ethernet port 2.
- *port-channel number*—Specifies a valid port-channel number. Range is 1-8.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the interface is specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Examples

The following example displays the COS configuration with no unit/port or port-channel parameter.

```
console#show interfaces cos-queue

Global Configuration
Interface Shaping Rate..................... 0

Queue Id   Min. Bandwidth   Scheduler Type   Queue Management Type
--------   --------------   --------------   ---------------------
0          0                Weighted         Tail Drop
1          0                Weighted         Tail Drop
2          0                Weighted         Tail Drop
3          0                Weighted         Tail Drop
4          0                Weighted         Tail Drop
5          0                Weighted         Tail Drop
6          0                Weighted         Tail Drop
```

This example displays the COS configuration for the specified interface 1/g1.

```
console#show interfaces cos-queue 1/g1
Interface.................................. 1/g1
Interface Shaping Rate..................... 0

Queue Id   Min. Bandwidth   Scheduler Type   Queue Management Type
--------   --------------   --------------   ---------------------
0          0                Weighted         Tail Drop
1          0                Weighted         Tail Drop
2          0                Weighted         Tail Drop
3          0                Weighted         Tail Drop
4          0                Weighted         Tail Drop
5          0                Weighted         Tail Drop
6          0                Weighted         Tail Drop
```

The following table lists the parameters in the examples and gives a description of each.

Parameter	Description
Interface	The port of the interface. If displaying the global configuration, this output line is replaced with a global configuration indication.
Intf Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth values in effect for the interface. This value is a configured value.
Queue Mgmt Type	The queue depth management technique used for all queues on this interface.
Queue	An interface supports *n* queues numbered 0 to (*n*-1).The specific *n* value is platform-dependent. Internal egress queue of the interface; queues 0–6 are available.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This value is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This value is a configured value.

show policy-map

Use the **show policy-map** command in Privileged EXEC mode to display all configuration information for the specified policy.

Syntax

show policy-map [*policyname*]

- *policyname*—Specifies the name of a valid existing DiffServ policy. (Range: 1-31)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DiffServ information.

```
console#show policy-map

Policy Name Policy Type Class Members

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

POLY1       xxx         DellClass

DELL        xxx         DellClass
```

show policy-map interface

Use the **show policy-map interface** command in Privileged EXEC mode to display policy-oriented statistics information for the specified interface.

Syntax

show policy-map interface *unit/port* **in**

- *unit/port*—Specifies a valid port number.

Default Configuration

This command has no default configuration.

Command Syntax

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the statistics information for port 1/g1.

```
console#show policy-map interface 1/g1 in

Interface..................................... 1/g1

Operational Status............................ Down

Policy Name................................... DELL

Interface Summary:
```

```
Class Name..................................... murali
In Discarded Packets........................... 0

Class Name..................................... test
In Discarded Packets........................... 0

Class Name..................................... DELL1
In Discarded Packets........................... 0

Class Name..................................... DELL
In Discarded Packets........................... 0
```

show service-policy

Use the **show service-policy** command in Privileged EXEC mode to display a summary of policy-oriented statistics information for all interfaces.

Syntax

show service-policy in

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of policy-oriented statistics information.

```
console#show service-policy

       Oper           Policy
Intf   Stat            Name
------ ----- ------------------------------
1/g1   Down  DELL
1/g2   Down  DELL
1/g3   Down  DELL
1/g4   Down  DELL
```

```
1/g5    Down   DELL
1/g6    Down   DELL
1/g7    Down   DELL
1/g8    Down   DELL
1/g9    Down   DELL
1/g10   Down   DELL
```

traffic-shape

Use the **traffic-shape** command in Global Configuration mode and Interface Configuration mode to specify the maximum transmission bandwidth limit for the interface as a whole. This process, also known as *rate shaping*, has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. To restore the default interface shaping rate value, use the **no** form of this command.

Syntax

traffic-shape *bw*

no traffic-shape

- *bw*—Maximum transmission bandwidth value expressed in terms of percentage. (Range: 0-100 percentage in increments of 5)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the setting of traffic-shape to a maximum bandwidth of 25.

```
console(config-if-1/g1)#traffic-shape 25
```

28

Radius Commands

auth-port

Use the **auth-port** command in Radius mode to set the port number for authentication requests of the designated Radius server.

Syntax

auth-port *auth-port-number*

- *auth-port-number*—Port number for authentication requests.

Default Configuration

The default value of the port number is 1812.

Command Mode

Radius mode

User Guidelines

The host is not used for authentication if set to 0.

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example sets the port number 2412 for authentication requests.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#auth-port 2412
```

deadtime

Use the **deadtime** command in Radius mode to improve Radius response times when a server is unavailable by causing the unavailable server to be skipped.

Syntax

deadtime *deadtime*

- *deadtime*—The amount of time that the unavailable server is skipped over. (Range: 0-2000 minutes)

Default Configuration

The default deadtime interval is 0 minutes.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies a deadtime interval of 60 minutes.

```
console(config)#radius-server host 192.143.120.123

console(config-radius)#deadtime 60
```

key

Use the **key** command in Radius mode to set the authentication and encryption key for all Radius communications between the switch and the Radius server.

Syntax

key *key-string*

- *key-string* —Specifies the authentication and encryption key for all Radius communications between the switch and the Radius server. This key must match the encryption used on the Radius. (Range: 0-128 characters)

Default Configuration

The default for *key-string* is an empty string.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies an authentication and encryption key of "*lion-king*".

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#key lion-king
```

priority

Use the **priority** command in Radius mode to specify the order in which the servers are to be used, with 0 being the highest priority.

Syntax

priority *priority*

- *priority*—Sets server priority level. (Range 0-65535)

Default Configuration

The default priority is 0.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies a priority of 10 for the designated server.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#priority 10
```

radius-server deadtime

Use the **radius-server deadtime** command in Global Configuration mode to improve Radius response times when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To set the deadtime to 0, use the **no** form of this command.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

- *deadtime*—Length of time in minutes, for which a Radius server is skipped over by transaction requests. (Range: 0 - 2000 minutes)

Default Configuration

The default dead time is 0 minutes.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the interval for which any unavailable Radius servers are skipped over by transaction requests to 10 minutes.

```
console(config)#radius-server deadtime 10
```

radius-server host

Use the **radius-server host** command in Global Configuration mode to specify a RADIUS server host and enter RADIUS Configuration mode. To delete the specified Radius host, use the **no** form of this command.

Syntax

radius-server host *{ip-address |hostname}*

no radius-server host *{ip-address |hostname}*

- *ip-address*—The R ADIUS server host IP address.
- hostname — Host name of the Radius server host. (Range: 1-158 characters)

Default Configuration

The parameters deadtime, key, source-ip, timeout and retransmit are set to the global values and the parameters auth-port-number, priority, usage are set to the default values 1812, 0 and **all**, respectively.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies a Radius server host with the following characteristics:

- Server host IP address—192.168.10.1

```
console(config)#radius-server host 192.168.10.1
```

radius-server key

Use the **radius-server key** command in Global Configuration mode to set the authentication and encryption key for all Radius communications between the switch and the Radius server. To reset to the default, use the **no** form of this command.

Syntax

radius-server key *[key-string]*

no radius-server key

- *key-string*—Specifies the authentication and encryption key for all Radius communications between the switch and the Radius server. This key must match the encryption used on the Radius server. (Range: 1-128 characters)

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the authentication and encryption key for all Radius communications between the device and the Radius server to "dell-server."

```
console(config)#radius-server key dell-server
```

radius-server retransmit

Use the **radius-server retransmit** command in Global Configuration mode to specify the number of times the Radius client will retransmit requests to the Radius server. To reset the default configuration, use the **no** form of this command.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

- *retries*—Specifies the retransmit value. (Range: 1 - 10)

Default Configuration

The default is 3 attempts.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the number of times the Radius client attempts to retransmit requests to the Radius server to 5 attempts.

```
console(config)#radius-server retransmit 5
```

radius-server source-ip

Use the **radius-server source-ip** command in Global Configuration mode to specify the source IP address used for communication with Radius servers. To return to the default, use the **no** form of this command. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

Syntax

radius-server source-ip *source*

no radius-server-ip

- *source*—Specifies the source IP address.

Default Configuration

The default IP address is the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the source IP address used for communication with Radius servers to 10.1.1.1.

```
console(config)#radius-server source-ip 10.1.1.1
```

radius-server timeout

Use the **radius-server timeout** command in Global Configuration mode to set the interval for which a switch waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

radius-server timeout *timeout*

no radius-server timeout

- *timeout*—Specifies the timeout value in seconds. (Range: 1 - 30)

Default Configuration

The default value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the interval for which a switch waits for a server host to reply to 5 seconds.

```
console(config)#radius-server timeout 5
```

retransmit

Use the **retransmit** command in Radius mode to specify the number of times the Radius client retransmits requests to the Radius server.

Syntax

retransmit *retries*

- *retries*—Specifies the retransmit value. (Range: 1-10 attempts)

Default Configuration

The default number for attempts is 3.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example of the retransmit command specifies five retries.

```
console(config)#radius-server host 192.143.120.123

console(config-radius)#retransmit 5
```

show radius-servers

Use the **show radius-servers** command in Privileged EXEC mode to display the Radius server settings.

Syntax

show radius-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the Radius server settings.

```
console#show radius-servers

IP address  Auth  TimeOut Retransmit  DeadTime  Source IP  Priority   Usage
----------- ----- ------- ---------- --------  --------  --------  -----
10.2.3.4    1812  6        Global    Global    0.0.0.0      0      all
10.240.1.4 1812  Global   Global    10        Global       0      all
```

```
Global Values
--------------
TimeOut : 3
Retransmit : 3
Deadtime : 0
Source IP : 1.2.3.4
```

source-ip

Use the **source-ip** command in Radius mode to specify the source IP address to be used for communication with Radius servers. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

Syntax

source-ip *source*

- *source*—A valid source IP address.

Default Configuration

The IP address is of the outgoing IP interface.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies 10.240.1.23 as the source IP address.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#source-ip 10.240.1.23
```

timeout

Use the timeout command in Radius mode to set the timeout value in seconds for the designated Radius server.

Syntax

timeout *timeout*

- *timeout*—Timeout value in seconds for the specified server. (Range: 1-30 seconds.)

Default Configuration

The default value is 3 seconds.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies the timeout setting for the designated Radius Server.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#timeout 20
```

usage

Use the **usage** command in Radius mode to specify the usage type of the server.

Syntax

usage *type*

- *type*—Variable can be one of the following values: *login*, *802.1x* or *all*.

Default Configuration

The default variable setting is *all*.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies usage type *login*.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#usage login
```

29

RMON Commands

rmon alarm

Use the **rmon alarm** command in Global Configuration mode to configure alarm conditions. To remove an alarm, use the **no** form of this command. Also see the related **show rmon alarm** command.

Syntax

rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

- *index*—The alarm index. (Range: 1 - 65535)
- *variable*—A fully qualified SNMP object identifier that resolves to a particular instance of an MIB object.
- *interval*—The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1 - 4294967295)
- *rthreshold*—Rising Threshold. (Range: 0 - 4294967295)
- *fthreshold*—Falling Threshold. (Range: 0 - 4294967295)
- *revent*—The index of the Event that is used when a rising threshold is crossed. (Range: 1-65535)
- *fevent*—The Event index used when a falling threshold is crossed. (Range: 1- 65535)
- **type** *type*—The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.

- **startup** *direction*—The alarm that may be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the *rthreshold*, and *direction* is equal to **rising** or **rising-falling**, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the *fthreshold*, and *direction* is equal to **falling** or **rising-falling**, then a single falling alarm is generated.
- **owner** *name*—Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

Default Configuration

The following parameters have the following default values:

- **type** *type*—If unspecified, the type is **absolute**.
- **startup** *direction*—If unspecified, the startup direction is **rising-falling**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the following alarm conditions:

- Alarm index—1
- Variable identifier—1.3.6.1.2.1.2.2.1.10.5
- Sample interval—10 seconds
- Rising threshold—500000
- Falling threshold—10
- Rising threshold event index—1
- Falling threshold event index—1

```
console(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.1.10.5 10 50000 10 1 1
```

rmon collection history

Use the **rmon collection history** command in Interface Configuration mode to enable a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command. Also see the **show rmon collection history** command.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

- *index*—The requested statistics index group. (Range: 1 - 65535)
- **owner** *ownername*—Records the RMON statistics group owner name. If unspecified, the name is an empty string.
- **buckets** *bucket-number*—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1 - 65535)
- **interval** *seconds*—The number of seconds in each polling cycle. If unspecified, defaults to 1800. (Range: 1 - 3600)

Default Configuration

The **buckets** configuration is 50. The **interval** configuration is 1800 seconds.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.

User Guidelines

This command cannot be executed on multiple ports using the **interface range ethernet** command.

Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on port 1/g8 with the index number "1" and a polling interval period of 2400 seconds.

```
console(config)#interface ethernet 1/g8

console(config-if-1/g8)#rmon collection history 1 interval 2400
```

rmon event

Use the **rmon event** command in Global Configuration mode to configure an event. To remove an event, use the **no** form of this command. Also see the **show rmon events** command.

Syntax

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

- *index*—The event index. (Range: 1 - 65535)
- *type*—The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.

- **community** *text*—If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- **description** *text*—A comment describing this event. (Range 0-127 characters)
- **owner** *name*—Enter a name that specifies who configured this event. If unspecified, the name is an empty string.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an event with the trap index of 10.

```
console(config)#rmon event 10 log
```

rmon table-size

Use the **rmon table-size** command in Global Configuration mode to configure the maximum RMON tables sizes. To return to the default configuration, use the **no** form of this command.

Syntax

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {**history** | **log**}

- **history** *entries*—Maximum number of history table entries. (Range: 20 - 270)
- **log** *entries*—Maximum number of log table entries. (Range: 20 - 100)

Default Configuration

History table size is 270.

Log table size is 200.

Command Mode

Global Configuration mode

User Guidelines

The configured table size is effective after the device is rebooted.

Example

The following example configures the maximum RMON history table sizes to 270 entries.

```
console(config)#rmon table-size history 270
```

show rmon alarm

Use the **show rmon alarm** command in User EXEC mode to display alarm configuration. Also see the **rmon alarm** command.

Syntax

show rmon alarm *number*

- *number*—Alarm index. (Range: 1 - 65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays RMON 1 alarms.

```
console> show rmon alarm 1

Alarm 1

-------

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type: delta

Startup Alarm: rising

Rising Threshold: 8700000

Falling Threshold: 78
```

```
Rising Event: 1
Falling Event: 1
Owner: CLI
```

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

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

show rmon alarm-table

Use the **show rmon alarm-table** command in User EXEC mode to display the alarms summary table.

Syntax

show rmon alarm-table

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the alarms summary table:

```
console> show rmon alarm-table

Index   OID                      Owner
-----   ------------------------ -------
1       1.3.6.1.2.1.2.2.1.10.1   CLI
2       1.3.6.1.2.1.2.2.1.10.1   Manager
3       1.3.6.1.2.1.2.2.1.10.9   CLI
```

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

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

show rmon collection history

Use the **show rmon collection history** command in User EXEC mode to display the requested group of statistics. Also see the **rmon collection history** command.

Syntax

show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—Valid Ethernet port. The full syntax is *unit* |*port*.
- *port-channel-number*—Valid trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all RMON group statistics.

```
console> show rmon collection history
Index  Interface  Interval   Requested  Granted  Owner
                              Samples   Samples
-----  --------- ---------- ---------- -------- -------
1        1/g1        30         50        50      CLI
2        1/g1       1800        50        50     Manager
```

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

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

show rmon events

Use the **show rmon events** command in User EXEC mode to display the RMON event table. Also see the **rmon event** command.

Syntax

show rmon events

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the RMON event table.

```
console> show rmon events

Index   Description     Type       Community  Owner   Last time sent
-----   -----------     --------- ---------- ------- ---------------------
1       Errors          Log                  CLI     Jan 18 2005  23:58:17
2       High Broadcast  Log-Trap   switch     Manager Jan 18 2005  23:59:48
```

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

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

show rmon history

Use the **show rmon history** command in User EXEC mode to display RMON Ethernet Statistics history. Also see the **rmon history** command.

Syntax

show rmon history *index* [**throughput** | **errors** | **other**] [**period** *seconds*]

- *index*—The requested set of samples. (Range: 1 - 65535)
- **throughput**—Displays throughput counters.
- **errors**—Displays error counters.
- **other**—Displays drop and collision counters.
- **period** *seconds*—Specifies the requested period time to display. (Range: 0 - 2147483647)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays RMON Ethernet Statistics history for "throughput" on index number 1.

```
console> show rmon history 1 throughput

Sample Set: 1 Owner: CLI

Interface:  1/g1 interval: 1800

Requested samples: 50       Granted samples: 50

Maximum table size: 270

Time                  Octets   Packets Broadcast Multicast   %

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

09-Mar-2005 18:29:32 303595962 357568     3289 7287         19

09-Mar-2005 18:29:42 287696304 275686     2789 5878         20
```

The following example displays RMON Ethernet Statistics history for errors on index number 1.

```
console> show rmon history 1 errors

Sample Set: 1                     Owner: Me

Interface:  1/g1                  interval: 1800
```

```
Requested samples: 50              Granted samples: 50

Maximum table size: 500 (800 after reset)


Time         CRC Align  Undersize  Oversize   Fragments  Jabbers

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

09-Mar-2005 1          1          0          49         0
18:29:32

09-Mar-2005 1          1          0          27         0
18:29:42
```

The following example displays RMON Ethernet Statistics history for "other" on index number 1.

```
console> show rmon history 1 other

Sample Set: 1               Owner: Me

Interface:  1/g1 Interval: 1800

Requested samples: 50       Granted samples: 50

Maximum table size: 270

Time                    Dropped   Collisions

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

10-Mar-2005  22:06:00      3           0

10-Mar-2005  22:06:20      3           0
```

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

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the Broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a Multicast address. This number does not include packets addressed to the Broadcast address.

Field	Description
%	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped. It is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

show rmon log

Use the **show rmon log** command in User EXEC mode to display the RMON logging table.

Syntax

show rmon log [*event*]

- *event*—Event index. (Range: 1 - 65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the RMON logging table.

```
console> show rmon log
Maximum table size: 100
Event Description    Time
----- -----------    --------------------
1     Errors         Jan 18 2005  23:48:19
1     Errors         Jan 18 2005  23:58:17
2     High Broadcast Jan 18 2005  23:59:48
console> show rmon log
Maximum table size: 100 (100 after reset)
Event Description    Time
----- -----------    --------------------
1     Errors         Jan 18 2005  23:48:19
1     Errors         Jan 18 2005  23:58:17
2     High Broadcast Jan 18 2005  23:59:48
```

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

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry was created.

show rmon statistics

Use the **show rmon statistics** command in User EXEC mode to display RMON Ethernet Statistics.

Syntax

show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}

- *interface*—Valid Ethernet unit/port.
- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays RMON Ethernet Statistics for port 1/g1.

```
console> show rmon statistics ethernet 1/g1

Port 1/g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

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

Field	Description
Dropped	The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, Broadcast packets, and Multicast packets) received.
Broadcast	The total number of good packets received and directed to the Broadcast address. This does not include Multicast packets.

Field	Description
Multicast	The total number of good packets received and directed to a Multicast address. This number does not include packets directed to the Broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

30

SNMP Commands

show snmp

Use the **show snmp** command in Privileged EXEC mode to display the SNMP communications status.

Syntax

show snmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SNMP communications status.

```
Console # show snmp
Community-String Community-Access View name     IP address
---------------- ---------------- ----------    ----------
public            read only        user-view      All
private           read write       Default        172.16.1.1
private           su               DefaultSuper   172.17.1.1
```

```
Community-String Group name  IP address
---------------- ---------   ----------
public           user-group   All

Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications
Target Address  Type    Community  Version  UDP  Filter TO  Retries
                                            Port name   Sec
-------------- ------  --------- -------  ---- ------ --- -----
192.122.173.42   Trap    public      2      162  filt1    15   3
192.122.173.42  Inform  public     2      162  filt2    15   3

Version 3 notifications
Target Address  Type  Username  Security  UDP  Filter  TO  Retries
                            Level    Port name   Sec
-------------- ----- --------  -------- ---- ------ --- ------
192.122.173.42  Inform   Bob     Priv    162  filt31 15    3
System Contact: Robert
System Location: Marketing
```

show snmp engineID

Use the **show snmp engineID** command in Privileged EXEC mode to display the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

show snmp engineID

Default Configuration

This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example displays the SNMP engine ID.

```
console# show snmp engineID

Local SNMP engineID: 08009009020C0B099C075878
```

show snmp filters

Use the **show snmp filters** command in Privileged EXEC mode to display the configuration of filters.

Syntax
show snmp filters *filtername*

- *filtername*—Specifies the name of the filter. (Range: 1-30)

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example

The following examples display the configuration of filters with and without a filter name specification.

```
console # show snmp filters
 Name                       OID Tree             Type
------------------- ----------------------------------
user-filter1          1.3.6.1.2.1.1             Included
user-filter1          1.3.6.1.2.1.1.7           Excluded
user-filter2          1.3.6.1.2.1.2.2.1.*.1     Included

console # show snmp filters user-filter1

Name                       OID Tree             Type
------------------- ----------------------------------
user-filter1          1.3.6.1.2.1.1             Included
user-filter1          1.3.6.1.2.1.1.7           Excluded
```

show snmp groups

Use the **show snmp groups** command in Privileged EXEC mode to display the configuration of groups.

Syntax

show snmp groups [*groupname*]

- *groupname*—Specifies the name of the group. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the configuration of views.

```
console# show snmp groups
    Name             Security                        Views
                   Model  Level          Read    Write    Notify
----------------- -----  ------        -------- -------- ------
user-group         V3    Auth-Priv     Default    ""       ""
managers-group     V3    NoAuth-priv   Default   Default   ""
managers-group     V3    NoAuth-priv   Default    ""       ""

console# show snmp groups user-group

    Name             Security                      Views
                     Model   Level           Read    Write    Notify
----------------- ------  ------        -------- -------- -------
user-group         V3    Auth-Priv     Default    ""       ""
```

The following table contains field descriptions.

Field	Description	
Name	Name of the group	
Security Model	SNMP model in use (v1, v2 or v3)	
Security Level	Authentication of a packet with encryption. Applicable only to SNMP Version 3 security model.	
Views	Read	A string that is the name of the view that enables you only to view the contents of the agent. If unspecified, all the objects except the community-table and SNMPv3 user and access tables are available.
	Write	A string that is the name of the view that enables you to enter data and manage the contents of the agent.

Field	Description	
	Notify	A string that is the name of the view that enables you to specify an inform or a trap

show snmp users

Use the **show snmp users** Privileged EXEC command to display the configuration of users.

Syntax

show snmp users [*username*]

- *username*—Specifies the name of the user. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the configuration of users with the user name specified.

```
Console # show snmp users
     Name          Group Name     Auth Priv
                                  Meth Meth    Remote Engine ID
--------------- --------------- ---- ---- -------------------
bob               user-group       MD5  DES  800002a20300fce3900106
john              user-group       SHA  DES  800002a20300fce3900106

Console # show snmp users bob
    Name           Group Name     Auth Priv
                                  Meth Meth   Remote Engine ID
--------------- --------------- ---- ---- -------------------
```

```
bob                 user-group       MD5  DES  800002a20300fce3900106
```

show snmp views

Use the **show snmp views** command in Privileged EXEC mode to display the configuration of views.

Syntax

show snmp views [*viewname*]

- *viewname*—Specifies the name of the view. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the configuration of views with and without a view name specified.

```
console# show snmp views


Name                 OID Tree          Type
-----------  ------------------------  ---------
user-view1   1.3.6.1.2.1.1             Included
user-view1   1.3.6.1.2.1.1.7           Excluded
user-view2   1.3.6.1.2.1.2.2.1.*.1     Included


console# show snmp views user-view1


Name         OID Tree                  Type
-----------  ------------------------  ----------------------------
user-view1   1.3.6.1.2.1.1             Included
user-view1   1.3.6.1.2.1.1.7           Excluded
```

snmp-server community

Use the **snmp-server community** command in Global Configuration mode to set up the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command. This Command places the user in SNMP-Community-Configuration mode.

Syntax

snmp-server community *community-string* {**ro** | **rw** | **su**} [**ipaddress** *ipaddress*] [**view** *viewname*]

no snmp-server community *community-string*

- *community-string*—Permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro**—Indicates read-only access
- **rw**—Indicates read-write access.

- **su**—Indicates SNMP administrator access.
- *ipaddress*—Specifies the IP address of the management station. If no IP address is specified, all management stations are permitted.
- *viewname*—Specifies the name of a previously defined view. For information on views, see the user guidelines. (Range: 1-30 characters)

Default Configuration

No community is defined.

Command Mode

Global Configuration mode

User Guidelines

You can not specify *viewname* for su, which has an access to the whole MIB. You can use the view name to restrict the access rights of a community string. When it is specified:

- An internal security name is generated.
- The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.
- The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view name. If **ro** is specified, then read-view and notify-view are mapped. If **rw** is specified, then read-view, notify-view, and write-view are mapped.

Example

The following example configures community access string **public** to permit administrative access to SNMP at an administrative station with IP address 192.168.1.20.

```
console(config)# snmp-server community public su 192.168.1.20
```

snmp-server community-group

Use the **snmp-server community-group** command in Global Configuration mode to map the internal security name for SNMP v1 and SNMP v2 security models to the group name. To remove the specified community string, use the **no** form of this command.

Syntax

snmp-server community-group *community-string group-name* [**ipaddress** *ip-address*]

- *community-string*—Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- *group-name*—Name of a previously defined group. The group defines the objects available to the community. (Range: 1-30 characters)

- ip-address—Management station IP address. Default is all IP addresses.

Default Configuration

No community group is defined.

Command Mode

Global Configuration mode

User Guidelines

The *group-name* parameter can be used to restrict the access rights of a community string. When it is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Example

The following example maps a community access string dell_community to group dell_group.

```
console(config)# snmp-server community-group dell_community
dell_group 192.168.29.1
```

snmp-server contact

Use the **snmp-server contact** command in Global Configuration mode to set up a system contact (sysContact) string. To remove the system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

- *text*—Character string, 0 to 160 characters, describing the system contact information.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays setting up the system contact point as "Dell_Technical_Support".

```
console(config)# snmp-server contact Dell_Technical_Support
```

snmp-server enable traps

Use the **snmp-server enable traps** command in Global Configuration mode to enable the switch to send SNMP traps. To disable SNMP traps use the **no** form of the command.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Configuration

Traps are enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the command to enable SNMP traps.

```
console(config)# snmp-server enable traps
```

snmp-server engineID local

Use the **snmpserver engineID local** command in Global Configuration mode to specify the Simple Network Management Protocol (SNMP) engine ID on the local device.

To remove the configured engine ID, use the **no** form of this command.

Syntax

snmp-server engineID local {*engineid-string* | **default** }

no snmp-server engineID local

- *engineid-string*—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. (Range: 5-32 characters)
- **default**—The engineID is created automatically, based on the device MAC address.

Default Configuration

The *engineID* is not configured.

Command Mode

Global Configuration mode

User Guidelines

If you want to use SNMPv3, you need to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device. If the SNMPv3 engine ID is deleted, or the configuration file is erased, then SNMPv3 cannot be used. Since the EngineID should be unique within an administrative domain, the following guidelines are recommended:

1) For standalone devices use the default keyword to configure the Engine ID.

2) For stackable systems, configure your own EngineID, and verify that is unique within your administrative domain.

Changing the value of snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

Example

The following example configures the Engine ID automatically.

```
console(config)# snmp-server engineID local default
```

snmp-server filter

Use the **snmp-server filter** command in Global Configuration mode to create or update a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the **no** form of this command.

Syntax

snmp-server filter *filter-name oid-tree* {**included | excluded**}

no snmp-server filter *filter-name* [*oid-tree*]

- *filter-name*—Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters.)
- *oid-tree*—Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as `1.3.6.2.4`, or a word, such as `system`. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, `1.3.*.4`.
- **included**—Indicates that the filter type is included.
- **excluded**—Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Examples

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
console(config)# snmp-server filter user-filter system included

console(config)# snmp-server filter user-filter system.7 excluded

console(config)# snmp-server filter user-filter ifEntry.*.1
included
```

snmp-server group

Use the **snmp-server group** command in Global Configuration mode to configure a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the **no** form of this command.

Syntax

snmp-server group *groupname* { **v1** | **v2** | **v3** { **noauth** | **auth** | **priv** } [**notify** *notifyview*] } [**context** *contextname*] [**read** *readview*] [**write** *writeview*]

no snmp-server group *groupname* { **v1** | **v2** | **v3** { **noauth** | **auth** | **priv** } } [**context** *contextname*]

- *groupname*—Specifies the name of the group. (Range: 1-30 characters.)
- **v1**—Indicates the SNMP Version 1 security model.
- **v2**—Indicates the SNMP Version 2 security model.
- **v3**—Indicates the SNMP Version 3 security model.
- **noauth**—Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- **auth**—Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- **priv**—Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- **noauth**—Specifies no authentication of a packet.
- *readview* —A string that is the name of the view that enables the you to view only the contents of the agent. If unspecified, all the objects except for the community-table and SNMPv3 user and access tables are available. (Range: 1-30 characters.)
- *writeview* —A string that is the name of the view that enables the user to enter data and configure the contents of the agent. If unspecified, nothing is defined for the write view. (Range: 1-30 characters.)
- *notifyview* —Defines a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. (Range: 1-30 characters.)

Default Configuration

No group entry exists. There will be some default groups for Read/Write/Super users. These groups cannot be deleted or modified by the user. This command is used only to configure the user-defined groups.

Command Mode

Global Configuration Mode

User Guidelines

View-name should be an existing view created using the **snmp-server view** command. If there are multiple records with the same view-name, then the argument specified in this command points to first view-name in the table.

Example

The following example attaches a group called **user-group** to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called **user-view**.

```
console(config)# snmp-server group user-group v3 priv read user-
view
```

snmp-server host

Use the **snmp-server host** command in Global Configuration mode to specify the recipient of Simple Network Management Protocol notifications. To remove the specified host, use the **no** form of this command. This command enters the user into SNMP-host configuration mode.

Syntax

snmp-server host {*ip-address* | *hostname*} *community* {**traps** {**v1** | **v2**} | **informs** [**timeout** *seconds*] [**retries** *retries*]} [**udpport** *port*] [**filter** *filtername*]

no snmp-server host *ip-address*

- *ip-address*—Specifies the IP address of the host (targeted recipient).
- *hostname*—Specifies the name of the host. (Range:1-158 characters)
- *community*—Specifies a password-like community string sent with the notification operation. (Range: 1-20 characters)
- **traps**—Indicates that SNMP traps are sent to this host.
- **v1**—Indicates that SNMPv1 traps will be used.
- **v2**—Indicates that SNMPv2 traps will be used.
- **informs**—Indicates that SNMPv2 informs are sent to this host.
- *seconds*—Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1-300 characters.)
- *retries*—Maximum number of times to resend an inform request. The default is 3 attempts. (Range: 1-255 characters.)
- *port*—UDP port of the host to use. The default is 162. (Range: 1-65535 characters.)
- *filtername*—A string that is the name of the filter that defines the filter for this host. If unspecified, does not filter anything (Range: 1-30 characters.)

Default Configuration

The default configuration is 3 retries, and 15 seconds timeout.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables SNMP traps for host 192.16.12.143.

```
console(config)# snmp-server host 192.16.12.143 Dell_powerconnect
traps v2
```

snmp-server location

Use the **snmp-server location** command in Global Configuration mode to set the system location string. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

- *text*—Character string describing the system location. (Range: 1 to 160 characters.)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the device location as "New_York".

```
console(config)# snmp-server location New_York
```

snmp-server trap authentication

Use the **snmp-server trap authentication** command in Global Configuration mode to enable the switch to send Simple Network Management Protocol traps when authentication fails. To disable SNMP failed authentication traps, use the **no** form of this command.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Configuration

Traps are enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the command to enable authentication failed SNMP traps.

```
console(config)# snmp-server trap authentication
```

snmp-server user

Use the **snmp-server user** command in Global Configuration mode to configure a new SNMP Version 3 user. To delete a user, use the **no** form of this command.

Syntax

snmp-server user *username groupname* [**remote** *engineid-string*] [{ **auth-md5** *password* | **auth-sha** *password* | **auth-md5-key** *md5-key* | **auth-sha-key** *sha-key* } [**priv-des** *password* | **priv-des-key** *des-key*]]

no snmp-server user *username*

- *username*—Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters.)
- *groupname*—Specifies the name of the group to which the user belongs. (Range: 1-30 characters.)

- *engineid-string*—Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. The remote engine id designates the remote management station, and should be defined to enable the device to receive acknowledgements to "informs." (Range: 5-32 characters.)
- **auth-md5**—The HMAC-MD5-96 authentication level. Enter a password. (Range: 8-64 characters.)
- **auth-sha**—The HMAC-SHA-96 authentication level. Enter a password. (Range: 8-64 characters.)
- *password*—A password. (Range: 1 to 32 characters.)
- **auth-md5-key**—The HMAC-MD5-96 authentication level. Enter a pregenerated MD5 key.
- **auth-sha-key**—The HMAC-SHA-96 authentication level. Enter a pregenerated SHA key.
- *md5-key*—Character string - length 32 hex characters.
- *sha-key*—Character string - length 48 characters.
- **priv-des**—The CBC-DES Symmetric Encryption privacy level. Enter a password.
- **priv-des-key**—The CBC-DES Symmetric Encryption privacy level. The user should enter a pregenerated MD5 or SHA key depending on the authentication level selected.
- *des-key*—The pregenerated DES encryption key. Length is determined by authentication method selected - 32 hex characters if MD5 Authentication is selected, 48 hex characters if SHA Authentication is selected.

Default Configuration

No user entry exists.

Command Mode

Global Configuration mode

User Guidelines

If the SNMP local engine ID is changed, configured users will no longer be able to connect and will need to be reconfigured.

Example

The following example configures an SNMPv3 user "John" in group "user-group".

```
console(config)# snmp-server user John user-group
```

snmp-server view

Use the **snmp-server view** command in Global Configuration mode to create or update a Simple Network Management Protocol (SNMP) server view entry. To delete a specified SNMP server view entry, use the **no** form of this command.

Syntax

snmp-server view *view-name oid-tree* { **included | excluded** }

no snmp-server view *view-name* [*oid-tree*]

- *view-name*—Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters.)
- *oid-tree*—Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as `1.3.6.2.4`, or a word, such as `system`. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example `1.3.*.4`.
- **included**—Indicates that the view type is included.
- **excluded**—Indicates that the view type is excluded.

Default Configuration

A view entry does not exist.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view record.

Examples

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.

```
console(config)# snmp-server view user-view system included
console(config)# snmp-server view user-view system.7 excluded
console(config)# snmp-server view user-view ifEntry.*.1 included
```

snmp-server v3-host

Use the **snmp-server v3-host** command in Global Configuration mode to specify the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server v3-host {*ip-address* | *hostname*} *username* {**traps** | **informs**} [**noauth** | **auth** | **priv**] [**timeout** *seconds*] [**retries** *retries*] [**udpport** *port*] [**filter** *filtername*]

no snmp-server host *ip-address*

- *ip-address*—Specifies the IP address of the host (targeted recipient).
- *hostname*—Specifies the name of the host. (Range:1-158 characters.)
- *username*—Specifies user name to use to generate the notification. (Range:1-25 characters.)
- **traps**—Indicates that SNMP traps are sent to this host.
- **informs**—Indicates that SNMPv2 informs are sent to this host.
- **noauth**—Specifies sending of a packet without authentication.
- **auth**—Specifies authentication of a packet without encrypting it
- **priv**—Specifies authentication and encryption of a packet.
- *seconds*—Number of seconds to wait for an acknowledgment before resending informs. This is not allowed for hosts configured to send traps. The default is 15 seconds. (Range:1-300 seconds.)
- *retries*—Maximum number of times to resend an inform request. This is not allowed for hosts configured to send traps. The default is 3 attempts. (Range:1-255 retries.)
- *port*—UDP port of the host to use. The default is 162. (Range:1-65535.)
- *filtername*—A string that is the name of the filter that define the filter for this host. If unspecified, does not filter anything. (Range:1-30 characters.)

Default Configuration

Default configuration is 3 retries and 15 seconds timeout.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example identifies an SNMPv3 host.

```
console(config)# snmp-server v3-host 192.168.0.20
```

31

Port Channel Commands

channel-group

Use the **channel-group** command in Interface Configuration mode to configure a port-to-port channel. To remove the channel-group configuration from the interface, use the **no** form of this command.

Syntax

channel-group *port-channel-number* **mode {on|auto}**

no channel-group

- *port-channel_number*—Specifies the number of the valid port-channel for the current port to join.
- **on**—Forces the port to join a channel without LACP.
- **auto**—Forces the port to join a channel with LACP.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how port 1/g5 is configured to port-channel number 1 without LACP.

```
console(config)# interface ethernet 1/g5

console(config-if-1/g5)# channel-group 1 mode on
```

interface port-channel

Use the **interface port-channel** command in Global Configuration mode to configure a port-channel type and enter port-channel configuration mode.

Syntax

interface port-channel *port-channel-number*

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

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the context of port-channel number 1.

```
console(config)# interface port-channel 1

console(config-if-ch1)#
```

interface range port-channel

Use the **interface range port-channel** command in Global Configuration mode to execute a command on multiple port channels at the same time.

Syntax

interface range port-channel {*port-channel-range*|**all**}

- *port-channel-range*—List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels. (Range: valid port-channel)
- **all**—All the channel-ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands in 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 stops the execution of the command on subsequent interfaces.

Example

The following example shows how port-channels 1, 2 and 8 are grouped to receive the same command.

```
console(config)# interface range port-channel 1-2,8
console(config-if)#
```

hashing-mode

Use the **hashing-mode** command to set the hashing algorithm on trunk ports.

Syntax

hashing-mode *mode*

- *mode*—Mode value in the range of 1 to 6.

  Range: 1–6:

  1. Source MAC, VLAN, EtherType, source module, and port ID
  2. Destination MAC, VLAN, EtherType, source module, and port ID
  3. Source IP and source TCP/UDP port
  4. Destination IP and destination TCP/UDP port
  5. Source/destination MAC, VLAN, EtherType, and source MODID/port
  6. Source/destination IP and source/destination TCP/UDP port

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (port-channel)

User Guidelines

No specific guidelines.

Example

```
console(config)#interface port-channel 1
```

```
console(config-if-ch1)#hashing-mode 4
```

no hashing-mode

Use the **no hashing-mode** command to set the hashing algorithm on Trunk ports to the default (3).

Syntax Description

no hashing-mode

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (port-channel)

User Guidelines

No specific guidelines.

Example

```
console(config)#interface port-channel 1

console(config-if-ch1)#no hashing mode
```

show interfaces port-channel

Use the **show interfaces port-channel** command to show port-channel information.

Syntax Description

show interfaces port-channel [*port-channel number*]

[*port-channel-number*]—Number of the port channel to show. This parameter is optional. If the port channel number is not given, all the channel groups are displayed. (Range: Valid port-channel number, 1 to 8)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
Console#show interfaces port-channel
Channel    Ports                                    Hashing-mode
-------    ---------------------------------------  ------------
 ch1       Active: 1/e1, 2/e2                       1
 ch2       Active: 2/e2, 2/e7 Inactive: 3/e1        2
 ch3       Active: 3/e3, 3/e8                       3 <default>
 ch4       No Configured Ports                      5
 ch5       No Configured Ports                      6
 ch6       No Configured Ports                      4
 ch7       No Configured Ports                      3 <default>
 ch8       No Configured Ports                      3 <default>

Hash algorithm type
1 - Source MAC, VLAN, EtherType, source module and port Id
2 - Destination MAC, VLAN, EtherType, source module and port Id
3 - Source IP and source TCP/UDP port
4 - Destination IP and destination TCP/UDP port
5 - Source/Destination MAC, VLAN, EtherType and source MODID/port
6 - Source/Destination IP and source/destination TCP/UDP port
```

show statistics port-channel

Use the **show statistics port-channel** command in Privileged EXEC mode to display statistics about a specific port-channel.

Syntax

show statistics port-channel *port-channel-number*

- *port-channel-number*—Valid port-channel number channel to display.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows statistics about port-channel 1.

```
console#show statistics port-channel 1
Total Packets Received (Octets)..... 0
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 1064
Packets RX and TX 65-127 Octets..... 140
Packets RX and TX 128-255 Octets..... 201
Packets RX and TX 256-511 Octets..... 418
Packets RX and TX 512-1023 Octets..... 1
Packets RX and TX 1024-1518 Octets..... 0
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0
Total Packets Received Without Errors..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
Broadcast Packets Received..... 0
Total Packets Received with MAC Errors..... 0
Jabbers Received..... 0
Fragments/Undersize Received..... 0
Alignment Errors..... 0
--More-- or (q)uit
FCS Errors..... 0
```

```
Overruns..................................... 0
Total Received Packets Not Forwarded.......... 0
Local Traffic Frames......................... 0
802.3x Pause Frames Received................. 0
Unacceptable Frame Type...................... 0
Multicast Tree Viable Discards............... 0
Reserved Address Discards.................... 0
Broadcast Storm Recovery..................... 0
CFI Discards................................. 0
Upstream Threshold........................... 0
Total Packets Transmitted (Octets)........... 263567
Max Frame Size............................... 1518
Total Packets Transmitted Successfully....... 1824
Unicast Packets Transmitted.................. 330
Multicast Packets Transmitted................ 737
Broadcast Packets Transmitted................ 757
Total Transmit Errors........................ 0
FCS Errors................................... 0
--More-- or (q)uit
Tx Oversized................................. 0
Underrun Errors.............................. 0
Total Transmit Packets Discarded............. 0
Single Collision Frames...................... 0
Multiple Collision Frames.................... 0
Excessive Collision Frames................... 0
Port Membership Discards..................... 0
802.3x Pause Frames Transmitted.............. 0
GVRP PDUs received........................... 0
GVRP PDUs Transmitted........................ 0
```

```
GVRP Failed Registrations..................... 0

Time Since Counters Last Cleared.............. 0 day 0 hr 17 min
52 sec

console#
```

32

Spanning Tree Commands

abort (mst)

Use the **abort** command in MST mode to exit the MST region configuration mode without applying the configuration changes.

Syntax

abort

Default Configuration

This command has no default configuration.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to exit the MST configuration mode without saving changes.

```
console(config)#spanning-tree mst configuration

console(config-mst)#abort
```

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** command in Privileged EXEC mode to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface*| **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet port. The full syntax is : *unit/port*.
- *port-channel-number*—A valid port channel.

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode

User Guidelines

This feature is used only when working in RSTP or MSTP mode.

Example

The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on 1/g1.

```
console#clear spanning-tree detected-protocols ethernet 1/g1
```

exit (mst)

Use the **exit** command in MST mode to exit the MST configuration mode and apply all configuration changes.

Syntax

exit

Default Configuration

MST configuration.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to exit the MST configuration mode and save changes.

```
console(config)#spanning-tree mst configuration
console(config-mst)#exit
```

instance (mst)

Use the **instance** command in MST mode to map VLANS to an MST instance.

Syntax

instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*

- *instance-ID*—ID of the MST instance. (Range: 1-15)
- *vlan-range*—VLANs to be added to the existing MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4093)

Default Configuration

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST mode

User Guidelines

Before mapping VLANs to an instance use the **spanning-tree mst enable** command to enable the instance.

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 switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
console(config)#spanning-tree mst configuration
console(config-mst)#instance 1 add vlan 10-20
```

name (mst)

Use the **name** command in MST mode to define the configuration name. To return to the default setting, use the **no** form of this command.

Syntax

name *string*

- *string*—Case sensitive MST configuration name. (Range: 1-32 characters)

Default Configuration

Bridge address.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the configuration name to "region1".

```
console(config)#spanning-tree mst configuration
console(config-mst)#name region1
```

revision (mst)

Use the **revision** command in MST mode to identify the configuration revision number. To return to the default setting, use the **no** form of this command.

Syntax

revision *value*

no revision

- *value*—Configuration revision number. (Range: 0-65535)

Default Configuration

Revision number is 0.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the configuration revision to 1.

```
console(config)#spanning-tree mst configuration
console(config-mst)#revision 1
```

show (mst)

Use the **show** command in MST mode to display the current or pending MST region configuration.

Syntax

show {current | pending}

- **current**—Current MST region configuration.
- **pending**—Pending MST region configuration. This setting is effective after exiting mst configuration context

Default Configuration

This command has no default configuration.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a pending MST region configuration.

```
console(config-mst)#show pending
Pending MST configuration
Name: Region1
Revision: 1
Instance        Vlans Mapped
--------        ------------
0               1-9,21-4094
1               10-20
```

show spanning-tree

Use the **show spanning-tree** command in Privileged EXEC mode to display the spanning-tree configuration.

Syntax

show spanning-tree [**ethernet** *interface-number* | **port-channel** *port-channel-number*] [**instance** *instance-id*]

show spanning-tree [**detail**] [**active** | **blockedports**] | [**instance** *instance-id*]

show spanning-tree mst-configuration

- **detail**—Displays detailed information.
- **active**—Displays active ports only.
- **blockedports**—Displays blocked ports only.
- **mst-configuration**—Displays the MST configuration identifier.
- *interface-number*—A valid Ethernet port number.
- *port-channel-number*—A valid port-channel index.
- *instance -id*—ID of the spanning -tree instance.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display spanning-tree information.

```
console#show spanning-tree
Spanning tree enabled mode RSTP
Root ID
            Address      00:01:42:97:e0:00
            Path Cost    20000
            Root Port    1 (1/g1)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID   Priority     36864
Address     00:02:4b:29:7a:00
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name       State    Prio.Nbr  Cost   Sts Role  PortFast
---------- -------  --------  ----   --- ----- ---------
1/g1       Enabled  128.1     20000  FWD Root  No
1/g2       Enabled  128.2     20000  FWD Desg  No
1/g3       Disabled 128.3     20000  -   -     -
1/g4       Enabled  128.4     20000  BLK Altn  No
1/g5       Enabled  128.5     20000  DIS -     -

console#show spanning-tree

Spanning tree enabled mode RSTP
Root ID
            Address      00:02:4b:29:7a:00
            This switch is the Root.
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name       State    Prio.Nbr  Cost  Sts  Role  PortFast
---------- -------  --------  ----  ---  ----- ---------
1/g1       Enabled  128.1     20000 FWD Desg   No
1/g2       Enabled  128.2     20000 FWD Desg   No
1/g3       Disabled 128.3     20000 -   -      -
1/g4       Enabled  128.4     20000 FWD Desg   No
1/g5       Enabled  128.5     20000 DIS -      -

console#show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Root ID
             Address     00:02:4b:29:7a:00
             Path Cost   20000
```

```
              Root Port   1(1/g1)
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID     Priority  36864
              Address   00:02:4b:29:7a:00
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces
Name       State    Prio.Nbr Cost  Sts Role  PortFast
---------- -------  -------- ----  --- ----- ---------
1/g1       Enabled  128.1    20000  -    -       -
1/g2       Enabled  128.2    20000  -    -       -
1/g3       Disabled 128.3    20000  -    -       -
1/g4       Enabled  128.4    20000  -    -       -
1/g5       Enabled  128.5    20000  -    -       -

console#show spanning-tree active
Spanning tree enabled mode RSTP

Root ID       Address 00:01:42:97:e0:00
              Path Cost    20000
              Root Port    1 (1/g1)
Hello Time 2 sec   Max Age 20 sec    Forward Delay 15 sec

Bridge ID     Priority     36864
              Address      00:02:4b:29:7a:00
Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

Interfaces
Name       State    Prio.Nbr  Cost  Sts  Role  PortFast
---------- -------  --------  ----  ---  ----- ---------
1/g1       Enabled  128.1     20000 FWD  Root  No
1/g2       Enabled  128.2     20000 FWD  Desg  No
```

```
1/g4       Enabled  128.4     20000 BLK  Altn  No

console#show spanning-tree blockedports
Spanning tree enabled mode RSTP

Root ID    Address   00:01:42:97:e0:00
           Path Cost 20000
           Root Port 1 (1/g1)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge   ID Priority     36864
         Address          00:02:4b:29:7a:00
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces
Name       State   Prio.Nbr Cost Sts Role  PortFast
---------- ------- -------- ---- --- ----- ---------
1/g4       Enabled 128.4    19   BLK Altn  No

console#show spanning-tree detail
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID     Address      00:01:42:97:e0:00
            Path Cost    20000
            Root Port    1 (1/g1)
            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, hello 2, max age 20, forward delay 15

Port 1 (1/g1) enabled
State: Forwarding                    Role: Root
Port id: 128.1                       Port cost: 20000
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
BPDU: sent 2, received 120638

Port 2 (1/g2) enabled
State: Forwarding                    Role: Designated
Port id: 128.2                       Port cost: 20000
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
BPDU: sent 2, received 170638

Port 3 (1/g3) enabled
State: Forwarding                    Role: Designated
Port id: 128.3                       Port cost: 20000
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
BPDU: sent 2, received 170638

Port 4 (1/g4) enabled
State: Blocking                       Role: Alternate
Port Identifier: 128.4                Port cost: 20000
Port Fast: No (configured:no)
Designated bridge Priority: 28672     Address: 00:30:94:41:62:c8
```

```
Designated port id: 128.25           Designated path cost: 20000
BPDU: sent 2, received 120638

console#show spanning-tree ethernet 1/g1
Port 1 (1/g1) enabled
State: Forwarding                     Role: Root
Port id: 128.1                        Port cost: 20000
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
BPDU: sent 2, received 120638

console#show spanning-tree mst-configuration
Name: Region1
Revision: 1
Instance    Vlan Mapped
----------  -------------------------------------------
 0          1, 5, 7
 1          3

console#show spanning-tree
Spanning tree enabled mode MSTP
######MST 0 Vlans Mapped: 1-9, 21-4094
Root ID      Address      00:01:42:97:e0:00
                 Path Cost    20000
                 Root Port    1 (1/g1)
                 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces
Name    State    Prio.Nbr Cost  Sts Role  PortFast
------- -------  -------- ----  --- ----- --------
1/g1    Enabled  128.1    20000 FWD Root  No
1/g2    Enabled  128.2    20000 FWD Desg  No
```

```
1/g3    Enabled  128.3    20000 FWD Desg  No
1/g4    Enabled  128.4    20000 FWD Desg  No

######MST 1 Vlans Mapped: 10-20
Root ID
                  Address       00:02:4b:29:89:76
                  Path Cost     20000
                  Root Port     4(1/g4)

Bridge ID         Priority      32768
                  Address       00:02:4b:29:7a:00

Interfaces
Name     State   Prio.Nbr Cost  Sts Role  PortFast
-------- ------- -------- ----  --- ----- ---------
1/g1     Enabled 128.1    20000 FWD Boun  No
1/g2     Enabled 128.2    20000 FWD Boun  No
1/g3     Enabled 128.3    20000 BLK Altn  No
1/g4     Enabled 128.4    20000 FWD Root  No

console#show spanning-tree detail
Spanning tree enabled mode MSTP
Default port cost method: long

######MST 0 Vlans Mapped: 1-9, 21-4094
Root ID      Priority     32768
                 Address      00:01:42:97:e0:00
                 Path Cost    20000
                 Root Port    1 (1/g1)
                 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Port 1 (1/g1) enabled
State: Forwarding                          Role: Root
```

```
Port id: 128.1                              Port cost: 20000
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
BPDU: sent 2, received 120638

Port 2 (1/g2) enabled
State: Forwarding                         Role: Designated
Port id: 128.2                            Port cost: 20000
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
BPDU: sent 2, received 170638

Port 3 (1/g3) enabled
State: Forwarding                         Role: Designated
Port id: 128.3                            Port cost: 20000
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
BPDU: sent 2, received 170638

Port 4 (1/g4) enabled
State: Forwarding                         Role: Designated
Port id: 128.4                            Port cost: 20000
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
BPDU: sent 2, received 170638

######MST 1 Vlans Mapped: 10-20
Root ID            Address       00:02:4b:29:89:76
```

```
                    Path Cost     20000
                    Port Cost     4 (1/g4)

Port 1 (1/g1) enabled
State: Forwarding                       Role: Boundary
Port id: 128.1                          Port cost: 20000
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
BPDU: sent 2, received 120638

Port 2 (1/g2) enabled
State: Forwarding                       Role: Designated
Port id: 128.2                          Port cost: 20000
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
BPDU: sent 2, received 170638

Port 3 (1/g3) disabled
State: Blocking                         Role: Alternate
Port id: 128.3                          Port cost: 20000
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
BPDU: sent 2, received 170638

Port 4 (1/g4) enabled
State: Forwarding                       Role: Designated
Port id: 128.4                          Port cost: 20000
Port Fast: No (configured:no)
Designated bridge Priority: 32768       Address: 00:02:4b:29:7a:00
Designated port id: 128.2               Designated cost: 20000
```

```
BPDU: sent 2, received 170638


console#show spanning-tree
Spanning tree enabled mode MSTP
######MST 0 Vlans Mapped: 1-9, 21-4094
 Root ID         Address           00:01:42:97:e0:00
                 Path Cost         20000
                 Root Port         1 (1/g1)
                 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

spanning-tree

Use the **spanning-tree** command in Global Configuration mode to enable spanning-tree functionality. To disable spanning-tree functionality, use the **no** form of this command.

Syntax

spanning-tree

no spanning-tree

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables spanning-tree functionality.

```
console(config)#spanning-tree
```

spanning-tree bpdu

Use the **spanning-tree bpdu** command in Global Configuration mode to define BPDU handling when the spanning-tree is disabled on an interface. Use the **no** form of this command to return to the default.

Syntax

spanning-tree bpdu {filtering | flooding}

no spanning-tree bpdu

- **filtering**—Filter BPDU packets when spanning-tree is disabled on an interface.
- **flooding**—Flood BPDU packets when spanning-tree is disabled on an interface.

Default Configuration

The default parameter value is **flooding**.

Command Mode

Global Configuration mode

User Guidelines

This command is relevant when spanning-tree is disabled globally or on a single interface.

Example

The following example defines BPDU packet flooding when spanning-tree is disabled on an interface**.**

```
console(config)#spanning-tree bpdu flooding
```

spanning-tree bpdu-protection

Use the **spanning-tree bpdu-protection** command in Global Configuration mode to enable BPDU protection on a switch. Use the **no** form of this command to resume the default status of BPDU protection function.

For an access layer device, the access port is generally connected to the user terminal (such as a PC) or file server directly and configured as an edge port to implement the fast transition. When the port receives a BPDU packet, the system sets it to non-edge port and recalculates the spanning tree, which causes network topology flapping. In normal cases, these ports do not receive any BPDU packets. However, someone may forge BPDU to maliciously attack the switch and cause network flapping.

RSTP provides BPDU protection function against such attack. After BPDU protection function is enabled on a switch, the system disables an edge port that has received BPDU and notifies the network manager about it. The disabled port can only be enabled by the **no** version of the command.

Syntax

spanning-tree bpdu-protection

no spanning-tree bpdu-protection

Default Configuration

BPDU protection is not enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables BPDU protection.

```
console(config)#spanning-tree bpdu-protection
```

spanning-tree cost

Use the **spanning-tree cost** command in Interface Configuration mode to configure the spanning-tree path cost for a port. To return to the default port path cost, use the **no** form of this command.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

- *cost*—The port path cost. (Range: 0 - 200,000,000)

Default Configuration

The default cost is 0, which signifies that the cost is automatically calculated based on port speed.

- **10G Port path cost—2000**
- **Port Channel**—20,000
- **1000 mbps (giga)**—20,000
- **100 mbps**—200,000
- **10 mbps**—2,000,000

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning-tree cost on 1/g5 to 35000.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#spanning-tree cost 35000
```

spanning-tree disable

Use the **spanning-tree disable** command in Interface Configuration mode to disable spanning-tree on a specific port. To enable spanning-tree on a port, use the **no** form of this command.

Syntax

spanning-tree disable

no spanning-tree disable

Default Configuration

By default, all ports are enabled for spanning-tree.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example disables spanning-tree on 1/g5.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#spanning-tree disable
```

spanning-tree forward-time

Use the **spanning-tree forward-time** command in Global Configuration mode 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.

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

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

- ***seconds***—Time in seconds. (Range: 4 - 30)

Default Configuration

The default forwarding-time for IEEE Spanning-tree Protocol (STP) is 15 seconds.

Command Modes

Global Configuration mode

User Guidelines

When configuring the Forward-Time the following relationship should be satisfied:

2*(Forward-Time - 1) >= Max-Age.

Example

The following example configures spanning-tree bridge forward time to 25 seconds.

```
console(config)#spanning-tree forward-time 25
```

spanning-tree hello-time

Use the **spanning-tree hello-time** command in Global Configuration mode to configure the spanning-tree bridge hello time, which is how often the switch broadcasts hello messages to other switches. To reset the default hello time, use the **no** form of this command.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree *hello-time*

- *seconds*—Time in seconds. (Range: 1 - 10)

Default Configuration

2 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the Hello-Time the following relationship should be satisfied:

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures spanning-tree bridge hello time to 5 seconds.

```
console(config)#spanning-tree hello-time 5
```

spanning-tree max-age

Use the **spanning-tree max-age** command in Global Configuration mode to configure the spanning-tree bridge maximum age. To reset the default maximum age, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds* -Time in seconds. (Range: 6 - 40)

Default Configuration

The default max-age for IEEE STP is 20 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the Max-Age the following relationships should be satisfied:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures the spanning-tree bridge maximum-age to 10 seconds.

```
console(config)#spanning-tree max-age 10
```

spanning-tree mode

Use the **spanning-tree mode** command in Global Configuration mode to configure the spanning-tree protocol. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mode {stp | rstp |mstp}

no spanning-tree mode

- **stp**—Spanning Tree Protocol (STP) is enabled.
- **rstp**—Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mstp**—Multiple Spanning Tree Protocol (MSTP) is enabled.

Default Configuration

Rapid Spanning Tree Protocol (RSTP) is supported.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode the switch would use STP when the neighbor switch is using STP. In MSTP mode the switch would use RSTP when the neighbor switch is using RSTP and would use STP when the neighbor switch is using STP.

Example

The following example configures the spanning-tree protocol to MSTP.

```
console(config)#spanning-tree mode mstp
```

spanning-tree mst configuration

Use the **spanning-tree mst configuration** command in Global Configuration mode to enable configuring an MST region by entering the multiple spanning-tree (MST) mode.

Syntax

spanning-tree mst configuration

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

For two or more switches 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 configures an MST region.

```
console (config)#spanning-tree mst configuration
console (config-mst)#instance 1 add vlan 10-20
console (config-mst)#name region1
console (config-mst)#revision 1
```

spanning-tree mst cost

Use the **spanning-tree mst cost** command in Interface Configuration mode to configure the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default port path cost, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

- *instance-ID*—ID of the spanning -tree instance. (Range: 1-15)
- *cost*—The port path cost. (Range: 0 - 200,000,000)

Default Configuration

The default value is 0, which signifies that the cost will be automatically calculated based on port speed.

The default configuration is:

- Ethernet (10 Mbps) - 2,000,000
- Fast Ethernet (100 Mbps) - 200,000
- Gigabit Ethernet (1000 Mbps) - 20,000
- Port-Channel - 20,000

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the MSTP instance 1 path cost for interface 1/g9 to 4.

```
console(config)#interface ethernet 1/g9
console(config-if-1/g9)#spanning-tree mst 1 cost 4
```

spanning-tree mst max-hops

Use the **spanning-tree mst priority** command in Global Configuration mode to configure the number of hops in an MST region before the Bridge Protocol Data Unit (BDPU) is discarded and the port information ages out. To return to the default setting, use the **no** form of this command.

Syntax

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

- *hop-count*—Number of hops in an MST region before the BDPU is discarded. (Range: 1-40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
console(config)#spanning-tree mst max-hops 10
```

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** command in Interface Configuration mode to configure port priority. To return to the default port priority, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

- *instance-ID*—ID of the spanning-tree instance. (Range: 1-16)
- *priority*—The port priority. (Range: 0 - 240 in multiples of 16)

Default Configuration

The default port-priority for IEEE MSTP is 128.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the port priority of port 1/g1 to 144.

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#spanning-tree mst 1 port-priority 144
```

spanning-tree mst priority

Use the **spanning-tree mst priority** command in Global Configuration mode to set the switch priority for the specified spanning-tree instance. To return to the default setting, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

- *instance-id*—ID of the spanning-tree instance. (Range: 1-16)
- *priority*—Sets the switch priority for the specified spanning-tree instance. This setting affects 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 bridge priority for IEEE STP 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 selected as the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
console(config)#spanning-tree mst 1 priority 4096
```

spanning-tree portfast

Use the **spanning-tree portfast** command in Interface Configuration mode to enable PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. To disable PortFast mode, use the **no** form of this command.

Syntax

spanning-tree portfast

no spanning-tree portfast

Default Configuration

PortFast mode is disabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This feature is to be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

An interface with PortFast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting the standard forward-time delay.

Example

The following example enables PortFast on 1/g5**.**

```
console(config)#interface ethernet 1/g5

console(config-if-1/g5)#spanning-tree portfast
```

spanning-tree port-priority

Use the **spanning-tree port-priority** command in Interface Configuration mode to configure port priority. To reset the default port priority, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority*—The port priority. (Range: 0 - 240)

Default Configuration

The default port-priority for IEEE STP 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 1/g5 to 96.

```
console(config)#interface ethernet 1/g5

console(config-if-1/g5)#spanning-tree port-priority 96
```

spanning-tree priority

Use the **spanning-tree priority** command in Global Configuration mode to configure the spanning-tree priority. The priority value is used to determine which bridge is elected as the root bridge. To reset the default spanning-tree priority use the **no** form of this command.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

- *priority*—Priority of the bridge. (Range: 0 - 61440)

Default Configuration

The default bridge priority for IEEE STP 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 spanning-tree priority to 12288.

```
console(config)#spanning-tree priority 12288
```

spanning-tree root-protection

Use the **spanning-tree root-protection** command in Interface Configuration mode to enable the Root protection function on a switch. Use the **no** form of this command to restore the default status of the Root protection function.

Due to configuration error of the maintenance personnel or a malicious user attack, a designated root of the network may receive a BPDU with higher priority and lose its status as a root, which causes undesired changes of network topology. Such unpermitted changes may pull the higher-speed traffic to lower-speed links and cause network congestion.

To avoid such a problem, RSTP provides a Root protection function. After being configured with Root protection, a port remains a designated port. Once this port receives a BPDU with higher priority, it turns to listening status and does not forward any packets (as if the link to it is disconnected). It resumes normal status if it receives no BPDU with higher-priority for a period of time.

Syntax

spanning-tree root-protection

no spanning-tree root-protection

Default Configuration

Root protection is not enabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the Root protection function on the switch.

```
console(config-if-1/g5)#spanning-tree root-protection
```

33

SSH Commands

crypto key generate dsa

Use the **crypto key generate dsa** command in Global Configuration mode to generate DSA key pairs for your switch. A key pair is one public DSA key and one private DSA key.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs: one public DSA key and one private DSA key. If your switch already has DSA keys when you issue this command, you are warned and prompted to replace the existing keys. The keys are not saved in the switch configuration; they are saved in the file system and the private key is never displayed to the user. DSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

Example

The following example generates DSA key pairs.

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

crypto key generate rsa

Use the **crypto key generate rsa** command in Global Configuration mode to generate RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs: one public RSA key and one private RSA key. If your switch already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys. The keys are not saved in the switch configuration; they are saved in the file system and the private key is never displayed to the user. RSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

Example

The following example generates RSA key pairs.

```
console(config)#crypto key generate rsa
```

crypto key pubkey-chain ssh

Use the **crypto key pubkey-chain ssh** command in Global Configuration mode to enter public key configuration mode in order to manually specify public keys such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Configuration

By default, this command has no public keys configured.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the SSH Public Key-chain configuration mode.

```
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob
console(config-pubkey-key)#key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
MuSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

ip ssh port

Use the **ip ssh port** command in Global Configuration mode to specify the TCP port to be used by the SSH server. To use the default port, use the **no** form of this command.

Syntax

ip ssh port *port-number*

no ip ssh port

- *port-number*—Port number for use by the SSH server. (Range: 1 - 65535)

Default Configuration

The default value is 22.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
console(config)#ip ssh port 8080
```

ip ssh pubkey-auth

Use the **ip ssh pubkey-auth** command in Global Configuration mode to enable public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration

The function is disabled.

Command Mode

Global Configuration mode

User Guidelines

AAA authentication is independent from this configuration.

Example

The following example enables public key authentication for incoming SSH sessions.

```
console(config)#ip ssh pubkey-auth
```

ip ssh server

Use the **ip ssh server command in** Global Configuration mode to enable the switch to be configured from SSH. To disable this function, use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Default Configuration

This command is **enabled** by default.

Command Mode

Global Configuration mode

User Guidelines

To generate SSH server keys, use the commands **crypto key generate rsa**, and **crypto key generate dsa**.

Example

The following example enables the switch to be configured using SSH.

```
console(config)#ip ssh server
```

key-string

Use the **key-string** SSH Public Key Configuration mode to specify an SSH public key manually.

Syntax

key-string *key-string*

key-string row *key-string*

- **row**—To specify the SSH public key row by row.
- *key-string*—The UU-encoded DER format is the same format as the authorized keys file used by OpenSSH.

Default Configuration

By default, the key-string is empty.

Command Mode

SSH Public Key Configuration mode

User Guidelines

Use the **key-string row** command to specify which SSH public key you will configure interactively next. To complete the interactive command, you must enter **key-string row** with no characters.

Examples

The following example shows how to enter a public key string for a user called "bob."

```
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
```

```
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#key-string row AAAAB3Nza
console(config-pubkey-key)#key-string row C1yc2
```

show crypto key mypubkey

Use the **show crypto key mypubkey** command in Privileged EXEC mode to display the SSH public keys of the switch.

Syntax

show crypto key mypubkey [**rsa**|**dsa**]

- **rsa**—RSA key.
- **dsa**—DSA key.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SSH public keys on the switch.

```
console#show crypto key mypubkey rsa
 rsa key data:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAu7WHtjQDUygjSQXHVgyqdUby
dxUXEAiDHXcWHVr0R/ak1HDQitBzeEv1vVEToEn5ddLmRhtIgRdKUJHgBHJV
```

```
R2VaSN/WC0IK53j9re4B11AE+O3qAxwJs0KD7cTkvF9I+YdiXeOM8VE4skkw
AiyLDNVWXgNQ6iat8+8Mjth+PIo5t3HykYUCkD8B1v93nzi/sr4hHHJCdx7w
wRW3QtgXaGwYt2rdlr3x8ViAF6B7AKYd8xGVVjyJTD6TjrCRRwQHgB/BHsFr
z/Rl1SYa0vFjel/7/0qaIDSHfHqWhajYkMa4xPOtIye7oqzAOm1b76l28uTB
luBEoLQ+PKOKMiK8sQ==

Fingerprint(hex): 58:7f:5c:af:ba:d3:60:88:42:00:b0:2f:f1:5a:a8:fc
Fingerprint(bubbleBabble): xodob-liboh-heret-tiver-dyrib-godac-pynah-
muzyt-mofim-bihog-cuxyx
```

show crypto key pubkey-chain ssh

Use the **show crypto key pubkey-chain ssh** command in Privileged EXEC mode to display SSH public keys stored on the switch.

Syntax

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint bubble-babble**|**hex**]

- *username*—Specifies the remote SSH client username. (Range: 1 - 48 characters)
- **bubble-babble**—Fingerprints in Bubble Babble format.
- **hex**—Fingerprint in Hex format. If fingerprint is unspecified, it defaults to Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all SSH public keys stored on the switch.

```
console#show crypto key pubkey-chain ssh

Username Fingerprint

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

bob      9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86

john     98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
```

The following example displays the SSH public called "dana."

```
console#show crypto key pubkey-chain ssh username dana
Username: dana

 rsa key data:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAywqRKTRnexccxVUVTeMl+Gkh
imyUDhcTkgEfssLPMsgoXlTwzCE5+97UIIsSRKQQWR+pBNl45tCYd75LUofV
4LP6Lj1Q5Q0w5lBgiqC2MZ/iBHGSsHMAE0lpYtelZprDu4uiZHMuWezmdQp9
a1PU4jwQ22TlcfaUq3sqC3FMUoU=
 Fingerprint: 2f:09:e7:6f:c9:bf:ab:04:d4:6f:a0:eb:e8:df:7a:11
```

show ip ssh

Use the **show ip ssh** command in Privileged EXEC mode to display the SSH server configuration.

Syntax

show ip ssh

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SSH server configuration.

```
console#show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:
IP Address         User Name                Idle Time       SessionTime
---------------    --------------------     -------------  -------------
10.240.1.122       John                     00:00:00        00:00:08
```

user-key

Use the **user-key** command in SSH Public Key Chain Configuration mode to specify which SSH public key you are configuring manually. To remove a SSH public key, use the **no** form of this command.

Syntax

user-key *username* {**rsa**|**dsa**}

no user-key *username*

- *username*—Specifies the remote SSH client username. (Range: 1 - 48 characters)
- **rsa**—RSA key
- **dsa**—DSA key

Default Configuration

By default, there are no keys.

Command Mode

SSH Public Key Chain Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables a SSH public key to be manually configured for the SSH public key chain called "bob."

```
console(config)#crypto key pubkey-chain ssh

console(config-pubkey-chain)#user-key bob rsa

console(config-pubkey-key)#
```

34

Syslog Commands

clear logging

Use the **clear logging** command in Privileged EXEC mode to clear messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears messages from the internal syslog message logging buffer.

```
console#clear logging

Clear logging buffer [y/n]
```

clear logging file

Use the **clear logging file** command in Privileged EXEC mode to clear messages from the logging file.

Syntax

clear logging file

Default Configuration

There is no default configuration for the command.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Example

The following example shows the **clear logging file** command and confirmation response.

```
console#clear logging file
Clear logging file [y/n]
```

description

Use the **description** command in Logging mode to describe the syslog server.

Syntax

description *description*

- *description*—Sets the description of the syslog server. (Range: 1-64 characters.)

Default Configuration

This command has no default value.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific syslog server, the command can be executed to set the description of the server.

Example

The following example sets the syslog server description.

```
console(config-logging)#description "syslog server 1"
```

level

Use the **level** command in Logging mode to specify the importance level of syslog messages. To reset to the default value, use the **no** form of the command.

Syntax

level *level*

no level

- *level*—The level number for syslog messages. (Range: **emergency, alert, critical, error, warning, notice, info, debug**)

Default Configuration

The default value for *level* is **info**.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific syslog server, the command can be executed to set the importance level for syslog messages.

Example

The following example sets the syslog message importance level to alert.

```
console(config-logging)#level alert
```

logging cli-command

Use the **logging cli-command** in Global Configuration mode to enable CLI command logging.

Syntax

logging cli-command

no logging cli-command

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

To see the CLI commands by using the **show logging** command.

Example

```
console(config)#logging cli-command
```

```
<189> JAN 13 05:20:27 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2113 %% CLI:EIA-

232:----:vlan 3

<189> JAN 13 05:20:27 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2114 %% CLI:EIA-

232:----:ex

<189> JAN 13 05:20:28 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2115 %% CLI:EIA-

232:----:

<189> JAN 13 05:20:39 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2116 %% CLI:EIA-

232:----:show logging file
```

logging

Use the **logging** command in Global Configuration mode to log messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

Syntax

logging {*ip-address* | *hostname*}

no logging {*ip-address* | *hostname*}

- *ip-address*—IP address of the host to be used as a syslog server.
- *hostname*—Hostname of the host to be used as a syslog server. (Range: 1-158 characters)

Default Configuration

No syslog servers defined.

Command Mode

Global Configuration mode

User Guidelines

Up to eight syslog servers can be used.

Example

The following example places the designated server in logging configuration mode.

```
console(config)#logging 192.168.15.1
```

logging buffered

Use the **logging buffered** command in Global Configuration mode to limit syslog messages displayed from an internal buffer based on severity. To cancel the buffer use, use the **no** form of this command.

Syntax

logging buffered *level*

no logging buffered

- *level*—Limits the message logging to a specified level buffer. (Range: **emergency, alert, critical, error, warning, notice, info, debug**)

Default Configuration

The default value for *level* is **info**.

Command Mode

Global Configuration mode

User Guidelines

All the syslog messages are logged to the internal buffer. This command limits the commands displayed to the user.

Example

The following example limits syslog messages displayed from an internal buffer based on the severity level "error".

```
console(config)#logging buffered error
```

logging buffered size

Use the **logging buffered size** command in Global Configuration mode to change the number of syslog messages stored in the internal buffer. To return the number of messages stored in the internal buffer to the default value, use the **no** form of this command.

Syntax

logging buffered size *number*

no logging buffered size

- *number*—Numeric value indicating the maximum number of messages stored in the history table. (Range: 20 - 400)

Default Configuration

The default number of messages is 200.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after reset.

Example

The following example changes the number of syslog messages stored in the internal buffer to 250.

```
console(config)#logging buffered size 250
```

logging console

Use the **logging console** command in Global Configuration mode to limit messages logged to the console based on severity. To disable logging to the console terminal, use the **no** form of this command.

Syntax

logging console *level*

no logging console

- *level*—Limits the logging of messages displayed on the console to a specified level. (Range: **emergency, alert, critical, error, warning, notice, info, debug**)

Default Configuration

The default value for *level* is **info**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example limits messages logged to the console based on severity level "alert".

```
console(config)#logging console alert
```

logging facility

Use the **logging facility** command in Global Configuration mode to set the facility for logging messages. To reset to the default value, use the **no** form of the command.

Syntax

logging facility *facility*

no logging facility

- *facility*—The facility that will be indicated in the message. (Range: local0, local1, local2, local3, local4, local5, local 6, local7)

Default Configuration

The default value is **local7**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the logging facility as **local3**.

```
console(config)#logging facility local3
```

logging file

Use the **logging file** command in Global Configuration mode to limit syslog messages sent to the logging file based on severity. To cancel the buffer, use the **no** form of this command.

Syntax

logging file *level*

no logging file

- *level*—Limits the logging of messages to the buffer to a specified level. (Range: **emergency, alert, critical, error, warning, notice, info, debug**)

Default Configuration

The default value for *level* is **error**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example limits syslog messages sent to the logging file based on the severity level "warning".

```
console(config)#logging file warning
```

logging on

Use the **logging on** command in Global Configuration mode to control error messages logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the **no** form of this command.

Syntax

logging on

no logging on

Default Configuration

Logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. Logging on and off for these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging <server>**global configuration commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example shows how logging is enabled.

```
console(config)#logging on
```

port

Use the **port** command in Logging mode to specify the port number of syslog messages. To reset to the default value, use the **no** form of the command.

Syntax

port *port*

no port

- port—The port number for syslog messages. (Range: 1-65535)

Default Configuration

The default port number is 514.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific syslog server, the command can be executed to set the port number for the server.

Example

The following example sets the syslog message port to 300.

```
console(config-logging)#port 300
```

show logging

Use the **show logging** command in Privileged EXEC mode to display the state of logging and the syslog messages stored in the internal buffer.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
console#show logging
```

```
Logging is enabled.

Console logging: level debugging. console Messages: 0 Dropped.

Buffer logging: level debugging. Buffer Messages: 11 Logged, 200
Max.

File logging: level notifications. File Messages: 0 Dropped.

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped.

console#show logging

Console logging: level warning. Console Messages: 2100 Dropped.

Buffer Logging: level info. Buffer Messages: 2100 Logged, 200 Max

File Logging: level notActive. File Messages: 0 Dropped.

CLI Command Logging : disabled

Web Session Logging : disabled

SNMP Set Command Logging : disabled

366 Messages were not logged.

Buffer Log:

<189> JAN 10 10:44:49 192.168.2.1-1 TRAPMGR[232224784]:
traputil.c(910) 1901 %% Spanning Tree Topology Change: 14, Unit: 1

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped.

2 messages were not logged (resources)

Buffer log:

11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface FastEthernet g1,
changed state to up

11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g1,
changed state to up

11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g1,
changed state to up

11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g2,
changed state to up

11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g3,
changed state to up

11-Aug-2005  15:41:43: %SYS-5-CONFIG_I: Configured from memory by
console
```

```
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet g1, changed state to up

11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down

11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down

11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g2, changed state to down

11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet 1/3, changed state to down
```

show logging file

Use the **show logging file** command in Privileged EXEC mode to display the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging and syslog messages sorted in the logging file.

```
console#show logging file

Persistent Logging : enabled

Persistent Log Count : 1

<186> JAN 01 00:00:05 0.0.0.0-1 UNKN[268434928]: bootos.c(382) 3
%% Event(0xaaaaaaaa)
```

show syslog-servers

Use the **show syslog-servers** command in Privileged EXEC mode to display the syslog servers settings.

Syntax

show syslog-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the syslog server settings.

```
console#show syslog-servers


IP address     Port Severity      Facility   Description
-------------- ---- ----------    --------    -----------
192.180.2.275  14   Info           local7      7
192.180.2.285  14   Warning        local7      7
```

35

TACACS+ Commands

key

Use the **key** command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon.

Syntax

key *key-string*

- key-string—To specify the key name. For an empty string use " ". (Range: 0 - 128 characters)

Default Configuration

If left unspecified, the key-string parameter defaults to the global value.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies an encryption and authentication key of 12.

```
console(config-tacacs)#key 12
```

port

Use the **port** command in TACACS Configuration mode to specify a server port number.

Syntax

port *port-number*

- *port-number*—The server port number. If left unspecified, the default port number is 49. (Range: 0 - 65535)

Default Configuration

The default port number is 49.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to specify server port number 1200.

```
console(tacacs)#port 1200
```

priority

Use the **priority** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority.

Syntax

priority *priority*

- *priority*—Specifies the priority for servers. 0 (zero) is the highest priority. (Range: 0 - 65535)

Default Configuration

If left unspecified, this parameter defaults to 0 (zero).

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to specify a server priority of 10000.

```
console(config-tacacs)#priority 10000
```

show tacacs

Use the **show tacacs** command in Privileged EXEC mode to display the configuration and statistics of a TACACS+ server.

Syntax

show tacacs [*ip-address*]

- *ip-address*—The name or IP address of the host.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays TACACS+ server settings.

```
console#show tacacs

Global Timeout: 5

IP address         Port    Timeout   Priority
---------------    -----   -------   --------
10.254.24.162      49      Global    0
```

tacacs-server host

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. To delete the specified hostname or IP address, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address*|*hostname*}

no tacacs-server host {*ip-address*|*hostname*}

- *ip-address*—The IP address of the TACACS+ server.
- *hostname*—The hostname of the TACACS+ server. (Range: 1-255 characters).

Default Configuration

No TACACS+ host is specified.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Example

The following example specifies a TACACS+ host.

```
console(config)#tacacs-server host 172.16.1.1

console(tacacs)#
```

tacacs-server key

Use the **tacacs-server key** command in Global Configuration mode to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. To disable the key, use the **no** form of this command.

Syntax

tacacs-server key *key-string*

no tacacs-server key

- *key-string*—Specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon. (Range: 0 - 128 characters)

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the authentication encryption key.

```
console(config)#tacacs-server key dell-s
```

tacacs-server timeout

Use the **tacacs-server timeout** command in Global Configuration mode to set the interval during which a switch waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

- *timeout*—The timeout value in seconds. (Range: 1 - 30)

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the timeout value as 30.

```
console(config)#tacacs-server timeout 30
```

timeout

Use the **timeout** command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used.

Syntax

timeout *timeout*

- *timeout*—The timeout value in seconds. (Range: 1 - 30)

Default Configuration

If left unspecified, the timeout defaults to the global value.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

This example shows how to specify the timeout value.

```
console(config-tacacs)#timeout 23
```

36

Telnet Server Commands

ip telnet server disable

This command is used to enable/disable the Telnet service on the switch.

ip telnet server disable

no ip telnet server disable

Syntax Description

Not applicable

Parameter Ranges

Not applicable

Command Mode

Global Configuration

Usage Guidelines

No specific guidelines.

Default Value

This feature is enabled by default.

Example

```
console#configure
console(config)#ip telnet server disable
console(config)# no ip telnet server disable
```

ip telnet port

This command is used to configure the Telnet service port number on the switch.

Syntax

ip telnet port *port number*

- *port number*—Telnet service port number (Range: 1–65535)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

Usage Guidelines

No specific guidelines.

Example

```
console(config)#ip telnet port 45
console(config)#no ip telnet port
```

show ip telnet

This command displays the status of the Telnet server and the Telnet service port number.

Syntax Description

show ip telnet

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

Example

```
(console)#show ip telnet
Telnet Server is Enabled. Port:23
```

37

VLAN Commands

dvlan-tunnel ethertype

Use the **dvlan-tunnel ethertype** command in Global Configuration mode to configure the ethertype for the specified interface.

To configure the EtherType on the specified interface to its default value, use the **no** form of this command.

Syntax

dvlan-tunnel ethertype {802.1Q | **vman** | **custom** <*0-65535*>}

no dvlan-tunnel ethertype

- 802.1Q—Configures the EtherType as 0x8100.
- vman—Configures the EtherType as 0x88A8.
- custom—Custom configures the EtherType for the DVLAN tunnel. The value must be 0-65535.

Default Configuration

The default for this command is 802.1Q.

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

Example

The following example displays configuring Double VLAN tunnel for vman EtherType.

```
console(config)#dvlan-tunnel ethertype vman
```

interface vlan

Use the **interface vlan** command in Global Configuration mode to configure a VLAN type and to enter Interface Configuration mode.

Syntax

interface vlan *vlan-id*

- *vlan-id*—The ID of a valid VLAN (Range: 0-4093).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

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

```
console(config)#interface vlan 1

console(config-vlan)#ip address 131.108.1.27 255.255.255.0
```

interface range vlan

Use the **interface range vlan** command in Global Configuration mode to execute a command on multiple VLANs at the same time.

Syntax

interface range vlan {*vlan-range*|*all*}

- *vlan-range*—A list of valid 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 - 4093)
- **all**—All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands used in the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution continues on other interfaces.

Example

The following example groups VLAN 221 till 228 and VLAN 889 to receive the same command.

```
console(config)#interface range vlan 221-228,889
console(config-if)#
```

mode dvlan-tunnel

Use the **mode dvlan-tunnel** command in Interface Configuration mode to enable Double VLAN Tunneling on the specified interface. To disable Double VLAN Tunneling on the specified interface, use the **no** form of this command.

Syntax

mode dvlan-tunnel

no mode dvlan-tunnel

Default Configuration

By default, Double VLAN Tunneling is *disabled*.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable Double VLAN Tunneling at ethernet port 1/g1.

```
console(config-if-1/g1)#mode dvlan-tunnel
```

name

Use the **name** command in Interface Configuration mode to add a name to a VLAN. To remove the VLAN name, use the **no** form of this command.

NOTE: This command cannot be configured for a range of interfaces (range context).

Syntax

name *string*

no name

- *string*—Comment or description to help identify a specific VLAN (Range: 1 - 32 characters).

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The VLAN name must be unique.

Example

The following example names VLAN number 19 with the name "Marketing."

```
console(config)#interface vlan 19
console(config-if-vlan19)#name Marketing
```

protocol group

Use the **protocol group** command in VLAN Database mode to attach a VLAN ID to the protocol-based group identified by *groupid*. A group may only be associated with one VLAN at a time. However, the VLAN association can be changed. The referenced VLAN should be created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To detach the VLAN from this protocol-based group identified by this *groupid*, use the **no** form of this command.

Syntax

protocol group *groupid vlanid*

no protocol group *groupid vlanid*

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.
- *vlanid*—A valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to attach the VLAN ID "100" to the protocol-based VLAN group "3."

```
console#vlan database
console(config-vlan)#protocol group 3 100
```

protocol vlan group

Use the **protocol vlan group** command in Interface Configuration mode to add the physical unit/port interface to the protocol-based group identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can be associated with one group only. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group. Ensure that the referenced VLAN is created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To remove the interface from this protocol-based VLAN group that is identified by this *groupid*, use the **no** form of this command.

If you select **all**, all ports are removed from this protocol group.

Syntax

protocol vlan group *groupid*

no protocol vlan group *groupid*

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add a physical port interface to the group ID of "2."

```
console(config-if-1/g1)#protocol vlan group 2
```

protocol vlan group all

Use the **protocol vlan group all** command in Global Configuration mode to add all physical interfaces to the protocol-based group identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can be associated with one group only. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group. Ensure that the referenced VLAN is created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To remove all interfaces from this protocol-based group that is identified by this *groupid*, use the **no** form of the command

Syntax

protocol vlan group all *groupid*

no protocol vlan group all *groupid*

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add all physical interfaces to the protocol-based group identified by group ID "2."

```
console(config)#protocol vlan group all 2
```

show dvlan-tunnel

Use the **show dvlan-tunnel** command in Privileged EXEC mode to display all interfaces enabled for Double VLAN Tunneling.

Syntax

show dvlan-tunnel *unit/port*

- *unit/port*—A valid unit and port number separated by forward slashes (/).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display all interfaces for Double VLAN Tunneling.

```
console#show dvlan-tunnel

Interfaces Enabled for DVLAN Tunneling..... 1/g1
```

show dvlan-tunnel interface

Use the **show dvlan-tunnel interface** command in Privileged EXEC mode to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Syntax

show dvlan-tunnel interface {*unit/port*|**all**}

- *unit/port*—A valid unit and port number separated by forward slashes (/).
- **all**—Displays information for all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays detailed information for unit/port "1/g1."

```
console#show dvlan-tunnel interface 1/g1

Interface Mode    EtherType
--------- ------- --------------
1/g1      Enable  vMAN
```

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

Field	Description
Mode	This field specifies the administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is *disabled*.
Interface	Interface Number.
EtherType	This field represents a 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. The three different EtherType tags are: (1) 802.1Q, which represents the commonly used value of 0x8100. (2) vMAN, which represents the commonly used value of 0x88A8. (3) If EtherType is not one of these two values, it is a custom tunnel value, representing any value in the range of 0 to 65535.

show interfaces switchport

Use the **show interfaces switchport** command in Privileged EXEC mode to display switchport configuration.

Syntax

show interfaces switchport {**ethernet** *interface*|**port-channel** *port-channel-number*}

- *Interface*—Specific interface, such as ethernet 1/g8.
- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays switchport configuration individually for g1.

```
console#show interface switchport ethernet 1/g1
Port 1/g1:
VLAN Membership mode: General

Operating parameters:
PVID: 1 (default)
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
Protected: Enabled

Port 1/g1 is member in:

VLAN      Name           Egress rule      Type
----      ---------      -----------      -----
1         default        untagged         Default
8         VLAN008        tagged           Dynamic
11        VLAN0011       tagged           Static
19        IPv6 VLAN      untagged         Static
72        VLAN0072       untagged         Static

Static configuration:
PVID: 1 (default)
Ingress Filtering: Enabled
Acceptable Frame Type: All

Port 1/g1 is statically configured to:

VLAN     Name           Egress rule
----     ---------      -----------
11       VLAN0011       tagged
19       IPv6 VLAN      untagged
72       VLAN0072       untagged

Forbidden VLANS:
VLAN     Name
----     ---------
73       Out
```

The following example displays switchport configuration individually for 1/g2.

```
console#show interface switchport ethernet 1/g2
Port 1/g2:
VLAN Membership mode: General

Operating parameters:
PVID: 4095 (discard vlan)
Ingress Filtering: Enabled
Acceptable Frame Type: All

Port 1/g1 is member in:
VLAN      Name           Egress rule     Type
----      ---------      -----------     -----
91        IP Telephony   tagged          Static

Static configuration:
PVID: 8
Ingress Filtering: Disabled
Acceptable Frame Type: All

Port 1/g2 is statically configured to:
VLAN     Name           Egress rule
----     ---------      -----------
8        VLAN0072       untagged
91       IP Telephony   tagged

Forbidden VLANS:
VLAN      Name
----      ---------
73        Out
```

The following example displays switchport configuration individually for 2/g19.

```
console#show interfaces switchport ethernet 2/g19
Port 2/g19:

Operating parameters:
PVID: 2922
Ingress Filtering: Enabled
Acceptable Frame Type: Untagged
GVRP status: Disabled

Port 2/g19 is member in:
VLAN      Name           Egress rule      Type
----      ---------      -----------      -----
2921      Primary A      untagged         Static
2922      Community A1   untagged         Static
```

```
Static configuration:
PVID: 2922
Ingress Filtering: Enabled
Acceptable Frame Type: Untagged
GVRP status: Disabled

Port 2/g19 is member in:
VLAN      Name           Egress rule      Type
----      ---------      -----------      -----
2921      Primary A      untagged         Static
2922      Community A1   untagged         Static
```

show port protocol

Use the **show port protocol** command in Privileged EXEC mode to display the Protocol-Based VLAN information for either the entire system or for the indicated group.

Syntax

show port protocol [*groupid* | **all**]

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command.
- **all**—Enter **all** to show all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the Protocol-Based VLAN information for either the entire system.

```
console#show port protocol all

                Group
Group Name       ID     Protocol(s) VLAN Interface(s)

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

test             1      IP          1    1/g1
```

show switchport protected

Use the **show switchport protected** command in Privileged EXEC mode to display the status of all the interfaces, including protected and unprotected interfaces.

Syntax

show switchport protected *groupid*

- *groupid*—Identifies which group the port is to be protected in. (Range: 0-2)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example identifies test as the protected group.

```
console#show switchport protected 0

Name..................................... test
```

show vlan

Use the **show vlan** command in Privileged EXEC mode to display VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- *vlan-id*—A valid VLAN ID.
- *vlan-name*—A valid VLAN name string. (Range: 1 - 32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all VLAN information.

```
console#show vlan
VLAN        Name               Ports       Type      Authorization
--------    ---------------    ------      -----     --------------
1           default            1/g1-1/g2   Other     Required
                               2/g1-1/g4
10          VLAN0010           1/g3-1/g4   dynamic   Required
11          VLAN0011           1/g1-1/g2   static    Required
20          VLAN0020           1/g3-1/g4   static    Required
21          VLAN0021                       static    Required
30          VLAN0030                       static    Required
31          VLAN0031                       static    Required
91          VLAN0011           1/g1-1/g2   static    Not Required
3964        Guest VLAN         1/g17       Guest     -
```

show vlan association mac

Use the **show vlan association mac** command in Privileged EXEC mode to display the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Syntax

show vlan association mac [*mac-address*]

- *mac-address*—Specifies the MAC address to be entered in the list. (Range: Any valid MAC address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows no entry in MAC address to VLAN cross-reference.

```
console#show vlan association mac


MAC Address               VLAN ID
```

```
-----------------------  -------
0001.0001.0001.0001      1


console#
```

show vlan association subnet

Use the **show vlan association subnet** command in Privileged EXEC mode to display the VLAN associated with a specific configured IP-Address and netmask. If no IP Address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Syntax

show vlan association subnet [*ip-address ip-mask*]

- *ip-address*—Specifies IP address to be shown
- *ip-mask*—Specifies IP mask to be shown

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The command has no user guidelines.

Example

The following example shows the case if no IP Subnet to VLAN association exists.

```
console#show vlan association subnet
IP Address       IP Mask          VLAN ID
---------------- ---------------- -------
The IP Subnet to VLAN association does not exist.
```

switchport access vlan

Use the **switchport access vlan** command in Interface Configuration mode to configure the VLAN ID when the interface is in access mode. To reconfigure the default, use the **no** form of this command.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

- *vlan-id*—A valid VLAN ID of the VLAN to which the port is configured.

Default Configuration

The default value for the *vlan-id* parameter is 1.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following example configures a VLAN ID of interface 1/g8 to become an access member of VLAN ID 23.

```
console(config)#interface ethernet 1/g8

console(config-if-1/g8)#switchport access vlan 23
```

switchport forbidden vlan

Use the **switchport forbidden vlan** command in Interface Configuration mode to forbid adding specific VLANs to a port. To revert to allowing the addition of specific VLANs to the port, use the **remove** parameter of this command.

Syntax

switchport forbidden vlan {**add** *vlan-list*|**remove** *vlan-list*}

- **add** *vlan-list*—List of valid VLAN IDs to add to the forbidden list. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

- **remove** *vlan-list*—List of valid VLAN IDs to remove from the forbidden list. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

All VLANs allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example forbids adding VLAN numbers 234 through 256 to port 1/g8.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#switchport forbidden vlan add 234-256
```

switchport general acceptable-frame-type tagged-only

Use the **switchport general acceptable-frame-type tagged-only** command in Interface Configuration mode to discard untagged frames at ingress. To enable untagged frames at ingress, use the **no** form of this command.

Syntax

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 1/g8 to discard untagged frames at ingress.

```
console(config)#interface ethernet 1/g8
```

```
console(config-if-1/g8)#switchport general acceptable-frame-type
tagged-only
```

switchport general allowed vlan

Use the **switchport general allowed vlan** command in Interface Configuration mode to add VLANs to or remove VLANs from a general port.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged**|**untagged**]

switchport general allowed vlan remove *vlan-list*

- **add** *vlan-list*—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove** *vlan-list*—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.
- **tagged**—Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged, the default is untagged.
- **untagged**—Sets the port to transmit untagged packets for the VLANs.

Default Configuration

Untagged.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

You can use this command to change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.

Example

The following example shows how to add VLANs 1, 2, 5, and 8 to the allowed list.

```
console(config-if-1/g8)#switchport general allowed vlan add
1,2,5,8 tagged
```

switchport general ingress-filtering disable

Use the **switchport general ingress-filtering disable** command in Interface Configuration mode to disable port ingress filtering. To enable ingress filtering on a port, use the **no** form of this command.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to enables port ingress filtering on 1/g8.

```
console(config)#interface ethernet 1/g8

console(config-if-1/g8)#switchport general ingress-filtering
disable
```

switchport general pvid

Use the **switchport general pvid** command in Interface Configuration mode to configure the Port VLAN ID (PVID) when the interface is in general mode. Use the **switchport mode general** command to set the VLAN membership mode of a port to "general." To configure the default value, use the **no** form of this command.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

- *vlan-id*—PVID. The VLAN ID may belong to a non-existent VLAN.

Default Configuration

The default value for the *vlan-id* parameter is 1 when the VLAN is enabled. Otherwise, the value is 4093.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to configure the PVID for 1/g8, when the interface is in general mode.

```
console(config)#interface ethernet 1/g8

console(config-if-1/g8)#switchport general pvid 234
```

switchport mode

Use the **switchport mode** command in Interface Configuration mode to configure the VLAN membership mode of a port. To reset the mode to the appropriate default for the switch, use the **no** form of this command.

Syntax

switchport mode {access|trunk|general}

no switchport mode

- **access**—An access port connects to a single end station belonging to a single VLAN. An access port is configured with ingress filtering enabled and will accept either an untagged frame or a packet tagged with the access port VLAN. An access port only egresses untagged packets.
- **trunk**—Trunk port connects two switches. A trunk port may belong to multiple VLANs. A trunk port accepts only packets tagged with the VLAN IDs of the VLANs to which the trunk is a member. A trunk only egresses tagged packets.
- **general**—Full 802.1q support VLAN interface. A general mode port may be a combination of both trunk and access ports. It is possible to fully configure all VLAN features on a general mode port.

Default Configuration

The default for this command is **access**.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 1/g8 to access mode.

```
console(config)#interface ethernet 1/g8

console(config-if-1/g8)#switchport mode access
```

switchport protected

Use the **switchport protected** command in Interface Configuration mode to configure a protected port. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group. You are required to remove an interface from one group before adding it to another group.

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Syntax

switchport protected *groupid*

no switchport protected

- *groupid*--Identifies which group this port will be protected in. (Range: 0-2)

Default Configuration

No protected switchports are defined.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures Ethernet port 1/g1 as a member of protected group 1.

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#switchport protected 1
```

switchport protected name

Use the **switchport protected name** command in Global Configuration mode to adds the port to the protected group 1 and also sets the group name to "protected".

Syntax

switchport protected *groupid* **name** *name*

no switchport protected *groupid* **name**

- *groupid*—Identifies which group the port is to be protected in. (Range: 0-2)
- *name*—Name of the group. (Range: 0-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example assigns the name "protected" to group 1.

```
console(config-if-1/g1)#switchport protected 1 name protected
```

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** command in Interface Configuration mode to add VLANs to or remove VLANs from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

- **add** *vlan-list*—List of VLAN IDs to add. Separate non-consecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove. Separate non-consecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to add VLANs 1, 2, and 5 to 8 to the allowed list.

```
console(config-if-1/g8)#switchport trunk allowed vlan add 1,2,5-8
```

vlan

Use the **vlan** command in VLAN Database mode to configure a VLAN. To delete a VLAN, use the **no** form of this command.

Syntax

vlan *vlan-range*

no vlan *vlan-range*

- *vlan-range*—A list of valid VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas (without spaces); use a hyphen to designate a range of IDs. (Range: 2 - 4093)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to create (add) VLAN of IDs 22, 23, and 56.

```
console(config-vlan)#vlan 22,23,56

console(config-vlan)#
```

vlan association mac

Use the **vlan association mac** command in VLAN Database mode to associate a MAC address to a VLAN.

Syntax

vlan association mac *mac-address vlanid*

no vlan association mac *mac-address*

mac-address—MAC address to associate. (Range: Any MAC address in the format xxxx.xxxx.xxxx)

vlanid—VLAN to associate with subnet. (Range: 1-4093)

Default Configuration
No assigned MAC address.

Command Mode
VLAN Database mode

User Guidelines
This command has no user guidelines.

Example
The following example associates MAC address with VLAN ID 1.

```
console(config-vlan)#vlan association mac 0001.0001.0001 1
```

vlan association subnet

Use the **vlan association subnet** command in VLAN Database mode to associate a VLAN to a specific IP-subnet.

Syntax
vlan association subnet *ip-address subnet-mask vlanid*

no vlan association subnet *ip-address subnet-mask*

- *ip-address*—Source IP address. (Range: Any valid IP address)
- *subnet-mask*—Subnet mask. (Range: Any valid subnet mask)
- *vlanid*—VLAN to associated with subnet. (Range: 1-4093)

Default Configuration
No assigned ip-subnet.

Command Mode
VLAN Database mode

User Guidelines
This command has no user guidelines.

Example
The following example associates IP address with VLAN ID 100.

```
console(config-vlan)#vlan association subnet 192.245.23.45
255.255.255.0 100
```

vlan database

Use the **vlan database** command in Global Configuration mode to enter the VLAN database configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the VLAN database mode.

```
console(config)#vlan database

console(config-vlan)#
```

vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Syntax

vlan makestatic *vlan-id*

- *vlan-id*—Valid vlan ID. Range is 2-4093.

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database Mode

User Guidelines

The dynamic VLAN (created via GRVP) should exist prior to executing this command. See the Type column in output from the **show vlan** command to determine that the VLAN is dynamic.

Example

The following changes vlan 3 to a static VLAN.

```
console(config-vlan)#vlan makestatic 3
```

vlan protocol group

Use the **vlan protocol group** command in Global Configuration mode to add protocol-based groups to the system. When a protocol group is created, it is assigned a unique group ID number. The group ID is used to identify the group in subsequent commands. Use the **no** form of the command to remove the specified VLAN protocol group name from the system.

Syntax

vlan protocol group *groupname*

no vlan protocol group *groupname*

- *groupname*—A character string that identifies the group name. (Range: 1 - 16 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

A Group ID is automatically generated when you create a protocol-based group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Example

The following example displays how to add the protocol-based group named "marketing."

```
console(config)#vlan protocol group marketing
```

vlan protocol group add protocol

Use the **vlan protocol group add protocol** command in Global Configuration mode to add a protocol to the protocol-based VLAN groups identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can be associated with one group only. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group.

To remove the protocol from the protocol-based VLAN group identified by *groupid*, use the **no** form of this command.

Syntax

vlan protocol group add protocol *groupid protocol*

no vlan protocol group add protocol *groupid protocol*

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.
- *protocol*—The protocol you want to add. (Range: *ip*, *arp*, and *ipx*)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add the "ip" protocol to the protocol based VLAN group identified as "2."

```
console(config)#vlan protocol group add protocol 2 ip
```

vlan protocol group remove

Use the **vlan protocol group remove** command in Global Configuration mode to remove the protocol-based VLAN group identified by *groupid*.

Syntax

vlan protocol group remove *groupid*

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the removal of the protocol-based VLAN group identified as "2."

```
console(config)#vlan protocol group remove 2
```

38

Web Server Commands

common-name

Use the **common-name** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the common-name for the switch.

Syntax

common-name *common-name*

- *common-name*—Specifies the fully qualified URL or IP address of the switch. If left unspecified, this parameter defaults to the lowest IP address of the switch (when the certificate is generated). (Range: 1 - 64)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certification mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the name of "router.gm.com."

```
console(config-crypto-cert)#common-name router.gm.com
```

country

Use the **country** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the country.

Syntax

country *country*

- *country*—Specifies the country name. (Range: 2 characters)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the country as "us."

```
console(config-crypto-cert)#country us
```

crypto certificate generate

Use the **crypto certificate generate** command in Global Configuration mode to generate a self-signed HTTPS certificate.

Syntax

crypto certificate *number* **generate**

- *number*—Specifies the certificate number. (Range: 1 - 2)
- **generate**—Regenerates the SSL RSA key.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command is not saved in the router switch configuration; however, the certificate and keys generated by this command are saved in the private configuration. This saved information is never displayed to the user or backed up to another switch. If the RSA keys do not exist, the **generate** parameter must be used.

Example

The following example generates a self-signed HTTPS certificate.

```
console(config)#crypto certificate 1 generate
console(config-crypto-cert)#
```

crypto certificate import

Use the **crypto certificate import** command in Global Configuration mode to import a certificate signed by the Certification Authority for HTTPS.

Syntax

crypto certificate *number* **import**

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

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enter an external certificate (signed by the Certification Authority) to the switch. To end the session, add a period (.) on a separate line after the input, and press ENTER.

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

If the public key found in the certificate does not match the switch's SSL RSA key, the command fails.

This command is not saved in the router configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another switch).

Example

The following example imports a certificate sighed by the Certification Authority for HTTPS.

```
console(config)#crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
```

```
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2005  to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

crypto certificate request

Use the **crypto certificate request** command in Privileged EXEC mode to generate and display a certificate request for HTTPS. This command takes you to Crypto Certificate Request mode.

Syntax

crypto certificate *number* **request**

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

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

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

Before generating a certificate request, you must first generate a self-signed certificate using the **crypto certificate generate** command in Global Configuration mode in order to generate the keys. Make sure to re-enter values in the certificate fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** command in Global Configuration mode to import the certificate into the switch. This certificate replaces the self-signed certificate.

Example

The following example generates and displays a certificate request for HTTPS.

```
console#crypto certificate 1 request

console(config-crypto-cert)#

-----BEGIN CERTIFICATE REQUEST-----

MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH

EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw

DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ

HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K

aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm

/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH

MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2

m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa

g+uNpyTkDt3ZVU72pjz/fa8TF0n3

-----END CERTIFICATE REQUEST-----

CN= router.gm.com

0= General Motors

C= US
```

duration

Use the **duration** command in Crypto Certificate Generation mode to specify the duration.

Syntax

duration *days*

- *days*—Specifies the number of days a certification would be valid. If left unspecified, the parameter defaults to 365 days. (Range: 30 - 3650 days)

Default Configuration

This command defaults to 365 days.

Command Mode

Crypto Certificate Generation mode

User Guidelines

This command mode is entered using the **crypto certificate request** command.

Example

The following example displays how specify a duration of 50 days that a certification is valid.

```
console(config-crypto-cert)#duration 50
```

ip http port

Use the **ip http port** command in Global Configuration mode to specify the TCP port for use by a web browser to configure the switch. To use the default TCP port, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

- *port-number*—Port number for use by the HTTP server. (Range: 0 - 65535)

Default Configuration

This default port number is 80.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines. However, specifying 0 as the port number effectively disables HTTP access to the switch.

Example

The following example shows how the http port number is configured to 100.

```
console(config)#ip http port 100
```

ip http server

Use the **ip http server** command in Global Configuration mode to enable the switch to be configured, monitored, or modified from a browser. To disable this function use the **no** form of this command.

Syntax

ip http server

no ip http server

Default Configuration

The default mode is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the switch to be configured from a browser.

```
console(config)#ip http server
```

ip https certificate

Use the **ip https certificate** command in Global Configuration mode to configure the active certificate for HTTPS. To return to the default setting, use the **no** form of this command .

Syntax

ip https certificate *number*

no ip https certificate

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

Default Configuration

The default value of the certificate number is 1.

Command Mode

Global Configuration mode

User Guidelines

The HTTPS certificate is generated using the **crypto certificate generate** command in Global Configuration mode.

Example

The following example configures the active certificate for HTTPS.

```
console(config)#ip https certificate 1
```

ip https port

Use the **ip https port** command in Global Configuration mode to configure a TCP port for use by a secure web browser to configure the switch. To use the default port, use the **no** form of this command.

Syntax

ip https port *port-number*

no ip https port

- *port-number*—Port number for use by the secure HTTP server. (Range: 1 - 65535)

Default Configuration

This default port number is 443.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the https port number to 100.

```
console(config)#ip https port 100
```

ip https server

Use the **ip https server** command in Global Configuration mode to enable the switch to be configured, monitored, or modified securely from a browser. To disable this function, use the **no** form of this command.

Syntax

ip https server

no ip https server

Default Configuration

The default for the switch is disabled.

Command Mode

Global Configuration mode

User Guidelines

You must use the **crypto certificate generate** command to generate the HTTPS certificate.

Example

The following example enables the switch to be configured from a browser.

```
console(config)#ip https server
```

key-generate

Use the **key-generate** command in Crypto Certificate Generation mode to specify the key-generate.

Syntax

key-generate [*length*]

- *length*—Specifies the length of the SSL's RSA key. If left unspecified, this parameter defaults to 1024. (Range: 512 - 2048)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation mode

User Guidelines

This command mode is entered using the **crypto certificate request** command.

Example

The following example displays how to specify that you want to regenerate the SSL RSA key 1024 byes in length.

```
console(config-crypto-cert)#key-generate 1024
```

location

Use the **location** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the location or city name.

Syntax

location *location*

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

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the city location of "austin."

```
console(config-crypto-cert)#location austin
```

organization-unit

Use the **organization-unit** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the organization unit.

Syntax

organization-unit *organization-unit*

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

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the "generalmotors" organization-unit.

```
console(config-crypto-cert)#organization-unit generalmotors
```

show crypto certificate mycertificate

Use the **show crypto certificate mycertificate** command in Privileged EXEC mode to view the SSL certificates of your switch.

Syntax

show crypto certificate mycertificate [*number*]

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

Default configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

Example

The following example displays the SSL certificate of a sample switch.

```
console#show crypto certificate mycertificate 1

-----BEGIN CERTIFICATE-----

dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS

NnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr

yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw

CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47

ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v

L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl

-----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

Finger print: DC789788 DC88A988 127897BC BB789788
```

show ip http

Use the **show ip http** command in Privileged EXEC mode to display the HTTP server configuration.

Syntax

show ip http

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC command

User Guidelines

This command has no user guidelines.

Example

The following example displays the HTTP server configuration.

```
console#show ip http

HTTP server enabled. Port: 80
```

show ip https

Use the **show ip http** command in Privileged EXEC mode to display the HTTPS server configuration.

Syntax

show ip https

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the HTTPS server configuration with DH Key exchange enabled.

```
console#show ip https

HTTPS server enabled. Port: 443
DH Key exchange enabled.
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
```

The following example displays the HTTPS server configuration with DH Key exchange disabled.

```
console#show ip https

HTTPS server enabled. Port: 443
DH Key exchange disabled, parameters are being generated.
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
```

state

Use the **state** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the state or province name.

Syntax

state *state*

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

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example shows how to specify the state of "texas."

```
console(config-crypto-cert)#state texas
```

39

Layer 3 Commands

The chapters that follow describe commands that conform to the OSI model's **Network Layer (Layer 3).** Layer 3 commands perform a series of exchanges over various data links to deliver data between any two nodes in a network. These commands define the addressing and routing structure of the Internet.

40

ARP Commands

arp

Use the **arp** command in Global Configuration mode to create an Address Resolution Protocol (ARP) entry. Use the **no** form of the command to remove the entry.

Syntax

arp *ip-address mac-address*

no arp *ip-address*

- *ip-address*—IP address of a device on a subnet attached to an existing routing interface.
- *mac-address*—A unicast MAC address for that device.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example creates an ARP entry consisting of an IP address and a MAC address.

```
console(config)#arp 192.168.1.2 00A2.64B3.A245
```

arp cachesize

Use the **arp cachesize** command in Global Configuration mode to configure the maximum number of entries in the ARP cache. To return the maximum number ARP cache entries to the default value, use the no form of this command.

Syntax

arp cachesize *integer*

no arp cachesize

- *integer*—Maximum number of ARP entries in the cache. (Range: 256-896)

Default Configuration

The default integer value is 896.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines an arp cachesize of 500.

```
console(config)#arp cachesize 500
```

arp dynamicrenew

Use the **arp dynamicrenew** command in Global Configuration mode to enable the ARP component to automatically renew dynamic ARP entries when they age out. To disable the automatic renewal of dynamic ARP entries when they age out, use the no form of the command.

Syntax

arp dynamicrenew

no arp dynamicrenew

Default Configuration

The default state is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console#configure
console(config)#arp dynamicrenew
```

```
console(config)#no arp dynamic renew
```

arp purge

Use the **arp purge** command in Privileged EXEC mode to cause the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Syntax

arp purge *ip-address*

- *ip-address*—The IP address to be removed from ARP cache.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example removes the specified IP address from arp cache.

```
console#arp purge 192.168.1.10
```

arp resptime

Use the **arp resptime** command in Global Configuration mode to configure the ARP request response timeout. To return the response timeout to the default value, use the no form of this command.

Syntax

arp resptime *integer*

no arp resptime

- *integer*—IP ARP entry response time out. (Range: 1-10 seconds)

Default Configuration

The default value is 1 second.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a response timeout of 5 seconds.

```
console(config)#arp resptime 5
```

arp retries

Use the **arp retries** command in Global Configuration mode to configure the ARP count of maximum requests for retries. To return to the default value, use the **no** form of this command.

Syntax

arp retries *integer*

no arp retries

- *integer*—The maximum number of requests for retries. (Range: 0-10)

Default Configuration

The default value is 4 retries.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines 6 as the maximum number of retries.

```
console(config)#arp retries 6
```

arp timeout

Use the **arp timeout** command in Global Configuration mode to configure the ARP entry ageout time. Use the no form of the command to set the ageout time to the default.

Syntax

arp timeout *integer*

no arp timeout

- *integer*—The IP ARP entry ageout time. (Range: 15-21600 seconds)

Default Configuration

The default value is 1200 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines 900 seconds as the timeout.

```
console(config)#arp timeout 900
```

clear arp-cache

Use the **clear arp-cache** command in Privileged EXEC mode to remove all ARP entries of type dynamic from the ARP cache.

Syntax

clear arp-cache [**gateway**]

- **gateway**—Removes the dynamic entries of type **gateway**, as well.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears all entries ARP of type dynamic, including gateway, from ARP cache.

```
console#clear arp-cache gateway
```

ip proxy-arp

Use the **ip proxy-arp** command in Interface Configuration mode to enable proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device

may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request. Use the no form of the command to disable proxy ARP on a router interface.

Syntax

ip proxy-arp

no ip proxy-arp

Default Configuration

Enabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables proxy arp for VLAN 15.

```
(config)#interface vlan 15
console(config-if-vlan15)#ip proxy-arp
```

show arp

Use the **show arp** command in Privileged EXEC mode to display the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the show ARP results in conjunction with the show ARP switch results.

Syntax

show arp [brief] [switch]

- brief—Display ARP parameters and cache.
- switch—Display ARP cache for the switch.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows **show arp** command output.

```
console#show arp
Age Time (seconds)..............................  1200
Response Time (seconds).........................  1
Retries.........................................  4
Cache Size......................................  896
Dynamic Renew Mode .............................  Enable
Total Entry Count Current / Peak ...............  1 / 1
Static Entry Count Configured / Active / Max ..  0 / 0 / 64

console#show arp switch

IP Address  MAC Address       Interface      Type     Age
----------- ----------------- -------------- -------- -----------

console#
```

41

DHCP and BOOTP Relay Commands

bootpdhcprelay cidridoptmode

Use the **bootpdhcprelay cidridoptmode** command in Global Configuration mode to enable the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system. Use the no form of the command to disable the circuit ID option and remote agent ID mode for BootP/DHCP Relay.

Syntax

bootpdhcprelay cidridoptmode

no bootpdhcprelay cidridoptmode

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the circuit ID and remote agent ID options.

```
console(config)#bootpdhcprelay cidridoptmode
Circuit Id and Remote Agent Id Mode set Successfully.
```

bootpdhcprelay enable

Use the **bootpdhcprelay** enable command in Global Configuration mode to enable the forwarding of relay requests for BootP/DHCP Relay on the system. Use the no form of the command to disable the forwarding of relay requests for BootP/DHCP Relay.

Syntax

bootpdhcprelay enable

no bootpdhcprelay enable

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console#configure
console(config)#bootpdhcprelay enable
console(config)#no bootpdhcprelay enable
```

bootpdhcprelay maxhopcount

Use the **bootpdhcprelay maxhopcount** command in Global Configuration mode to configure the maximum allowable relay agent hops for BootP/DHCP Relay on the system. Use the no form of the command to set the maximum hop count to the default value.

Syntax

bootpdhcprelay maxhopcount *integer*

no bootpdhcprelay maxhopcount

- *integer*—Maximum allowable relay agent hops for BootP/DHCP Relay on the system. (Range: 1-16)

Default Configuration

The default *integer* configuration is 4.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a maximum hopcount of 6.

```
console(config)#bootpdhcprelay maxhopcount 6
```

bootpdhcprelay minwaittime

Use the **bootpdhcprelay minwaittime** command in Global Configuration mode to configure the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it might use the seconds-sinceclient- began-booting field of the request as a factor in deciding whether to relay the request or not. Use the no form of the command to set the minimum wait time to the default value.

Syntax

bootpdhcprelay minwaittiime *integer*

no bootpdhcprelay minwaittime

- *integer*—Minimum wait time for BootP/DHCP Relay on the system. (Range: 0-100 seconds)

Default Configuration

0 is the default *integer* configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a minimum wait time of 10 seconds.

```
console(config)#bootpdhcprelay minwaittime 10
```

bootpdhcprelay serverip

Use the **bootpdhcprelay serverip** command in Global Configuration mode to configure the server IP address for BootP/DHCP Relay on the system. Use the no form of the command to set the IP address to the default value. Use the no form of the command to return the server IP address to the default value.

Syntax

bootpdhcprelay serverip *ip-address*

no bootpdhcprelay serverip

- *ip-address*—IP address of the BootP/DHCP Relay server

Default Configuration

0.0.0.0 is the default *ip-address*.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines the BootP/DHCP Relay server IP address.

```
console(config)#bootpdhcprelay serverip 192.168.30.3
```

show bootpdhcprelay

Use the **show bootpdhcprelay** command in User EXEC mode to display the BootP/DHCP Relay information.

Syntax

show bootpdhcprelay

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example defines the BootP/DHCP Relay information.

```
console>show bootpdhcprelay

Maximum Hop Count.............................. 6

Minimum Wait Time(Seconds)..................... 0

Admin Mode..................................... Enable

Server IP Address.............................. 192.168.30.3
```

```
Circuit Id and Remote Agent ID Option Mode..... Enable
Requests Received.............................. 0
Requests Relayed............................... 0
Packets Discarded.............................. 0
```

42

DHCPv6 Commands

clear ipv6 dhcp

Use the **clear ipv6 dhcp** command in Privileged EXEC mode to clear DHCPv6 statistics for all interfaces or for a specific interface.

Syntax

clear ipv6 dhcp {statistics | interface vlan *vlan-id* **statistics}**

- *vlan-id*—Valid VLAN ID.
- **statistics**—Indicates statistics display if VLAN is specified.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples clears DHCPv6 statistics for VLAN 11.

```
console#clear ipv6 dhcp interface vlan 11 statistics
```

dns-server

Use the **dns-server** command in IPv6 DHCP Pool Configuration mode to set the ipv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server. DNS server address is configured for stateless server support.

Syntax

dns-server *dns-server-address*

no dns-server *dns-server-address*

- *dns-server-address*—Valid IPv6 address.

Default Configuration

This command has no default configuration.

Command Mode

IPv6 DHCP Pool Configuration mode

User Guidelines

DHCPv6 pool can have multiple number of domain names with maximum of 8.

Example

The following example sets the ipv6 DNS server address of 2020:1::1, which is provided to a DHCPv6 client by the DHCPv6 server.

```
console(config)#ipv6 dhcp pool addrpool

console(config-dhcp6s-pool)#dns-server 2020:1::1
```

domain-name

Use the **domain-name** command in IPv6 DHCP Pool Configuration mode to set the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server. DNS domain name is configured for stateless server support.

Syntax

domain-name *dns-domain-name*

no domain-name *dns-domain-name*

- *dns-domain-name*—DHCPv6 domain name. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

IPv6 DHCP Pool Configuration mode

User Guidelines

DHCPv6 pool can have multiple number of domain names with maximum of 8.

Example

The following example sets the DNS domain name "test", which is provided to a DHCPv6 client by the DHCPv6 server.

```
console(config)#ipv6 dhcp pool addrpool

console(config-dhcp6s-pool)#domain-name test

console(config-dhcp6s-pool)#no domain-name test
```

ipv6 dhcp pool

Use the **ipv6 dhcp pool** command in Global Configuration mode to enter IPv6 DHCP Pool Configuration mode. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Syntax

ipv6 dhcp pool *pool-name*

no ipv6 dhcp pool *pool-name*

- *pool-name*—DHCPv6 pool name. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters IPv6 DHCP Pool Configuration mode.

```
console(config)#ipv6 dhcp pool addrpool

console(config-dhcp6s-pool)#
```

ipv6 dhcp relay

Use the **ipv6 dhcp relay** command in Interface Configuration mode to configure an interface for DHCPv6 relay functionality.

Syntax

ipv6 dhcp relay {**destination** *relay-address* [**interface vlan** *vlan-id*] | **interface vlan** *vlan-id*}[**remote-id** {**duid-ifid** | *user-defined-string*}]

- **destination**—Keyword that sets the relay server IPv6 address.
- *relay-address*—An IPv6 address of a DHCPv6 relay server.
- **interface**—Sets the relay server interface.
- *vlan-id*—A valid VLAN ID.
- [**remote-id** {**duid-ifid**|*user-defined-string*}]—The Relay Agent Information Option "remote ID" sub-option to be added to relayed messages. This can either be the special keyword duid-ifid, which causes the "remote ID" to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel) mode

User Guidelines

If *relay-address* is an IPv6 global address, then *relay-interface* is not required. If *relay-address* is a link-local or multicast address, then *relay-interface* is required. Finally, a value for *relay-address* is not specified, then a value for *relay-interface* must be specified and the DHCPV6-ALLAGENTS multicast address (i.e. FF02::1:2) is used to relay DHCPv6 messages to the relay server.

Example

The following example configures VLAN 15 for DHCPv6 relay functionality.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 dhcp relay destination 2020:1::1
```

ipv6 dhcp relay-agent-info-opt

Use **ipv6 dhcp relay-agent-info-opt** command in Global Configuration mode to configure a number to represent the DHCPv6 Relay Agent Information Option. The DHCPv6 Relay Agent Information Option allows for various sub-options to be attached to messages that are being relayed by the local router to a relay server. The relay server may in turn use this information in determining an address to assign to a DHCPv6 client.

Syntax

ipv6 dhcp relay-agent-info-opt *option*

- *option*—Agent information option. (Range: 32-65535)

Default Configuration

32 is the default value for *option*.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the number 100 to represent the DHCPv6 Relay Agent Information Option.

```
console(config)#ipv6 dhcp relay-agent-info-opt 100
```

ipv6 dhcp relay-agent-info-remote-id-subopt

Use the **ipv6 dhcp relay-agent-info-remote-id-subopt** command in Global Configuration mode to configure a number to represent the DHCPv6 the "remote-id" sub-option.

Syntax

ipv6 dhcp relay-agent-info-remote-id-subopt *suboption*

- *suboption*—Remote ID suboption. (Range: 1-65535)

Default Configuration

1 is the default value for *suboption*.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the number 100 to represent the DHCPv6 the "remote-id" sub-option.

```
console(config)#ipv6 dhcp relay-agent-info-remote-id-subopt 100
```

ipv6 dhcp server

Use the **ipv6 dhcp server** command in Interface Configuration mode to configure DHCPv6 server functionality on an interface. For a particular interface DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Syntax

ipv6 dhcp server *pool-name* [**rapid-commit**] [**preference** *pref-value*]

- *pool-name*—The name of the DHCPv6 pool containing stateless and/or prefix delegation parameters
- **rapid-commit**—Is an option that allows for an abbreviated exchange between the client and server.
- *pref-value*—Preference value - used by clients to determine preference between multiple DHCPv6 servers. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures DHCPv6 server functionality.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 dhcp server pool
```

prefix-delegation

Use the **prefix-delegation** command in IPv6 DHCP Pool Configuration mode to define Multiple IPv6 prefixes within a pool for distributing to specific DHCPv6 Prefix delegation clients.

Syntax

prefix-delegation *prefix/prefixlength DUID* [**name** *hostname*] [**valid-lifetime** *valid-lifetime*] [**preferred-lifetime** *preferred-lifetime*]

no prefix-delegation *prefix/prefixlength*

- *prefix/prefixlength*—Delegated IPv6 prefix.

- *DUID*—Client DUID (e.g. 00:01:00:09:f8:79:4e:00:04:76:73:43:76').
- *hostname*—Client hostname used for logging and tracing. (Range: 0-31 characters.)
- *valid-lifetime*—Valid lifetime for delegated prefix. (Range: 0-4294967295 seconds)
- *preferred-lifetime*—Preferred lifetime for delegated prefix. (Range: 0-4294967295 seconds)

Default Configuration

2592000 seconds is the default value for *preferred-lifetime*. 604800 seconds is the default value for *valid-lifetime*.

Command Mode

IPv6 DHCP Pool Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a Multiple IPv6 prefix and client DUID within a pool for distributing to specific DHCPv6 Prefix delegation clients.

```
console(config)#ipv6 dhcp pool addrpool

console(config-dhcp6s-pool)#prefix-delegation 2020:1::1/64
00:01:00:09:f8:79:4e:00:04:76:73:43:76
```

service dhcpv6

Use the **service dhcpv6** command in Global Configuration mode to enable DHCPv6 configuration on the router.

Syntax

service dhcpv6

no service dhcpv6

Default Configuration

Enabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables DHCPv6 globally.

```
console#configure
console(config)#service dhcpv6
console(config)#no service dhcpv6
```

show ipv6 dhcp

Use the **show ipv6 dhcp** command in Privileged EXEC mode to display the DHCPv6 server name and status.

Syntax

show ipv6 dhcp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DHCPv6 server name and status.

```
console#show ipv6 dhcp
DHCPv6 is disabled
Server DUID:
```

show ipv6 dhcp binding

Use the **show ipv6 dhcp binding** command in Privileged EXEC mode to display the configured DHCP pool.

Syntax

show ipv6 dhcp binding [*ipv6-addr*]

- *ipv6-addr*—Valid IPv6 address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the configured DHCP pool based on the entered IPv6 address.

```
console#show ipv6 dhcp binding 2020:1::
```

show ipv6 dhcp interface

Use the **show ipv6 dhcp interface** command in User EXEC mode to display DHCPv6 information for all relevant interfaces or a specified interface. If an interface is specified, the optional statistics parameter is available to view statistics for the specified interface.

Syntax

show ipv6 dhcp interface vlan *vlan-id* [**statistics**]

- *vlan-id*—Valid VLAN ID.
- **statistics**—Enables statistics display if interface is specified.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display DHCPv6 information for VLAN 11.

```
console> show ipv6 dhcp interface vlan 11

IPv6 Interface.............................. vlan11

Mode........................................ Relay
```

```
Relay Address.................................. 2020:1::1
Relay Interface Number......................... Relay
Relay Remote ID.............................
Option Flags................................

console> show ipv6 dhcp interface vlan 11 statistics
DHCPv6 Interface vlan11 Statistics
-----------------------------------
DHCPv6 Solicit Packets Received................ 0
DHCPv6 Request Packets Received................ 0
DHCPv6 Confirm Packets Received................ 0
DHCPv6 Renew Packets Received.................. 0
DHCPv6 Rebind Packets Received................. 0
DHCPv6 Release Packets Received................ 0
DHCPv6 Decline Packets Received................ 0
DHCPv6 Inform Packets Received................. 0
DHCPv6 Relay-forward Packets Received.......... 0
DHCPv6 Relay-reply Packets Received............ 0
DHCPv6 Malformed Packets Received.............. 0
Received DHCPv6 Packets Discarded.............. 0
Total DHCPv6 Packets Received.................. 0
DHCPv6 Advertisement Packets Transmitted....... 0
DHCPv6 Reply Packets Transmitted............... 0
DHCPv6 Reconfig Packets Transmitted............ 0
DHCPv6 Relay-reply Packets Transmitted......... 0
DHCPv6 Relay-forward Packets Transmitted....... 0
Total DHCPv6 Packets Transmitted............... 0
```

show ipv6 dhcp pool

Use the **show ipv6 dhcp pool** command in Privileged EXEC mode to display the configured DHCP pool.

Syntax

show ipv6 dhcp pool *pool-name*

- *pool-name*—Name of the pool. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the configured DHCP pool.

```
console#show ipv6 dhcp pool test

DHCPv6 Pool: test
```

show ipv6 dhcp statistics

Use the **show ipv6 dhcp statistics** command in User EXEC mode to display the DHCPv6 server name and status.

Syntax

show ipv6 dhcp statistics

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DHCPv6 server name and status.

```
console> show ipv6 dhcp statistics
DHCPv6 Interface Global Statistics
-----------------------------------
DHCPv6 Solicit Packets Received..... 0
DHCPv6 Request Packets Received..... 0
DHCPv6 Confirm Packets Received..... 0
DHCPv6 Renew Packets Received..... 0
DHCPv6 Rebind Packets Received..... 0
DHCPv6 Release Packets Received..... 0
DHCPv6 Decline Packets Received..... 0
DHCPv6 Inform Packets Received..... 0
DHCPv6 Relay-forward Packets Received..... 0
DHCPv6 Relay-reply Packets Received..... 0
DHCPv6 Malformed Packets Received..... 0
Received DHCPv6 Packets Discarded..... 0
Total DHCPv6 Packets Received..... 0
DHCPv6 Advertisement Packets Transmitted..... 0
DHCPv6 Reply Packets Transmitted..... 0
DHCPv6 Reconfig Packets Transmitted..... 0
DHCPv6 Relay-reply Packets Transmitted..... 0
DHCPv6 Relay-forward Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```

43

DVMRP Commands

ip dvmrp

Use the **ip dvmrp** command to set the administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Syntax

ip dvmrp

no ip dvmrp

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets VLAN 15's administrative mode of DVMRP to active.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip dvmrp
```

ip dvmrp metric

Use the **ip dvmrp metric** command in Interface Configuration mode to configure the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network.

Syntax

ip dvmrp metric *metric*

no ip dvmrp metric

- *metric*—Cost to reach the network. (Range: 1-31)

Default Configuration

1 the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a metric of 5 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip dvmrp metric 5
```

ip dvmrp trapflags

Use the **ip dvmrp trapflags** command in Global Configuration mode to enable the DVMRP trap mode.

Syntax

ip dvmrp trapflags

no ip dvmrp trapflags

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following command enables DVMRP trap mode.

```
console#configure
console(config)#ip dvmrp trapflags
console(config)#no ip dvmrp trapflags
```

show ip dvmrp

Use the **show ip dvmrp** command in Privileged EXEC mode to display the system-wide information for DVMRP.

Syntax

show ip dvmrp

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide information for DVMRP.

```
console(config)#show ip dvmrp
Admin Mode..................................... Disable
Version........................................ 3
Total Number of Routes......................... 0
Reachable Routes .............................. 0
          DVMRP INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
```

show ip dvmrp interface

Use the **show ip dvmrp interface** command in Privileged EXEC mode to display the interface information for DVMRP on the specified interface.

Syntax

show ip dvmrp interface *vlan-id*

- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays interface information for VLAN 11 DVMRP.

```
console(config)#show ip dvmrp interface vlan 11

Interface Mode.............................. Disable
```

show ip dvmrp neighbor

Use the **show ip dvmrp neighbor** command in Privileged EXEC mode to display the neighbor information for DVMRP.

Syntax

show ip dvmrp neighbor

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the neighbor information for DVMRP.

```
console(config)#show ip dvmrp neighbor

No neighbors available.
```

show ip dvmrp nexthop

Use the **show ip dvmrp nexthop** command in Privileged EXEC mode to display the next hop information on outgoing interfaces for routing multicast datagrams.

Syntax

show ip dvmrp nexthop

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the next hop information on outgoing interfaces for routing multicast datagrams.

```
console(config)#show ip dvmrp nexthop

                                 Next Hop
Source IP       Source Mask      Interface Type
--------------- ---------------- --------- -------
```

show ip dvmrp prune

Use the **show ip dvmrp prune** command in Privileged EXEC mode to display the table that lists the router's upstream prune information.

Syntax

show ip dvmrp prune

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the table that lists the router's upstream prune information.

```
console(config)#show ip dvmrp prune

                                                    Expiry
Group           IP Source       IP Source Mask  Time(secs)
--------------- --------------- --------------- --------------
```

show ip dvmrp route

Use the **show ip dvmrp route** command in Privileged EXEC mode to display the multicast routing information for DVMRP.

Syntax

show ip dvmrp route

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast routing information for DVMRP.

```
console#show ip dvmrp route

              Upstream                  Expiry     Up Time
Source Address Neighbor Interface Metric Time(secs) (secs)
-------------- -------- --------------- ----------  ---------
```

44

IGMP Commands

ip igmp

Use the **ip igmp** command in Global Configuration mode to set the administrative mode of IGMP in the system to active.

Syntax

ip igmp

no ip igmp

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables IGMP.

```
console(config)#ip igmp
```

ip igmp last-member-query-count

Use the **ip igmp last-member-query-count** command in Interface Configuration mode to set the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.

Syntax

ip igmp last-member-query-count *count*

no ip igmp last-member-query-count

- *count*—Query count. (Range: 1-20)

Default Configuration

The default last member query count is 2.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets 10 as the number of VLAN 2 Group-Specific Queries.

```
console#configure
console(config)#interface vlan 2
console(config-if-vlan2)#ip igmp last-member-query-count 10
console(config-if-vlan2)#no ip igmp last-member-query-count
```

ip igmp last-member-query-interval

Use the **ip igmp last-member-query-interval** command in Interface Configuration mode to configure the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.

Syntax

ip igmp last-member-query-interval *tenthsofseconds*

no ip igmp last-member-query-interval

- *tenthsofseconds*—Maximum Response Time in tenths of a second (Range: 0-255)

Default Configuration

10 is the default Maximum Response Time value in tenths of a second.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 2 seconds as the Maximum Response Time inserted in VLAN 15's Group-Specific Queries.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp last-member-query-interval 20
```

ip igmp query-interval

Use the **ip igmp query-interval** command in Interface Configuration mode to configure the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

- *seconds*—Query interval. (Range: 1-3600)

Default Configuration

125 seconds is the default query interval value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 10-second query interval for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp query-interval 10
```

ip igmp query-max-response-time

Use the **ip igmp query-max-response-time** command in Internet Configuration mode to configure the maximum response time interval for the specified interface. It is the maximum query response time advertised in IGMPv2 queries on this interface. The time interval is specified in tenths of a second.

Syntax

ip igmp query-max-response-time *tenthsofseconds*

no ip igmp query-max-response-time

- *tenthsofseconds*—Maximum response time. (Range: 0-255 seconds)

Default Configuration

100 tenths of seconds is the default maximum response time value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a maximum response time interval of one second for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp query-max-response-time 10
```

ip igmp robustness

Use the **ip igmp robustness** command in Interface Configuration mode to configure the robustness that allows tuning of the interface, that is, tuning for the expected packet loss on a subnet. If a subnet is expected to have significant loss, the robustness variable may be increased for the interface.

Syntax

ip igmp robustnest *robustness*

no ip igmp robustnest

- *robustness*—Robustness variable. (Range: 1-255)

Default Configuration

2 is the default robustness value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a robustness value of 10 for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp robustness 10
```

ip igmp startup-query-count

Use the **ip igmp startup-query-count** command in Interface Configuration mode to set the number of queries sent out on startup - at intervals equal to the startup query interval for the interface.

Syntax

ip igmp startup-query-count *count*

no ip igmp startup-query-count

- *count*—The number of startup queries. (Range: 1-20)

Default Configuration

2 is the default count value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets for VLAN 15 the number of queries sent out on startup at 10 .

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp startup-query-count 10
```

ip igmp startup-query-interval

Use the **ip igmp startup-query-interval** command in Interface Configuration mode to set the interval between general queries sent at startup on the interface.

Syntax

ip igmp startup-query-interval *seconds*

no ip igmp startup-query-interval

- *seconds*—Startup query interval. (Range: 1-300 seconds)

Default Configuration

31 seconds is the default interval value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets at 10 seconds the interval between general queries sent at startup for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp startup-query-interval 10
```

ip igmp version

Use the **ip igmp version** command in Interface Configuration mode to configure the version of IGMP for an interface.

Syntax

ip igmp version *version*

- *version*—IGMP version. (Range: 1-3)

Default Configuration

3 is the default version.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures version 2 of IGMP for VLAN 15.

```
console#interface vlan 15
console(config-if-vlan15)#ip igmp version 2
```

show ip igmp

Use the **show ip igmp** command in Privileged EXEC mode to display system-wide IGMP information.

Syntax

show ip igmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide IGMP information .

```
console#show ip igmp groups vlan 2
IP Address..................................... 1.1.1.1
Subnet Mask.................................... 255.255.255.0
Interface Mode................................. Enable
Querier Status................................. Querier
```

show ip igmp groups

Use the **show ip igmp groups** command in Privileged EXEC mode to display the registered multicast groups on the interface. If **detail** is specified, this command displays the registered multicast groups on the interface in detail.

Syntax

show ip igmp groups vlan *vlan-id* [**detail**]

- *vlan-id*—Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the registered multicast groups for VLAN 1.

```
console(config)#show ip igmp groups vlan 1

IP Address..................................... 0.0.0.0

Subnet Mask.................................... 0.0.0.0
```

show ip igmp interface

Use the **show ip igmp interface** command in Privileged EXEC mode to display the IGMP information for the specified interface.

Syntax

show ip igmp interface vlan *vlan-id*

- *vlan-id*—Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IGMP information for VLAN 11.

```
console#show ip igmp vlan 11

Interface..................................... 11

IGMP Admin Mode............................... Enable
```

```
Interface Mode.............................. Enable
IGMP Version................................ 3
Query Interval (secs)....................... 125
Query Max Response Time (1/10 of a second)..... 100
Robustness.................................. 2
Startup Query Interval (secs) ................ 31
Startup Query Count......................... 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count...................... 2
```

show ip igmp interface membership

Use the **show ip igmp interface membership** command in Privileged EXEC mode to display the list of interfaces that have registered in the multicast group. If **detail** is specified, this command displays detailed information about the listed interfaces

Syntax

show ip igmp interface membership *groupaddr* [**detail**]

- *groupaddr*—Group IP address

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display the list of interfaces that have registered in the multicast group at IP address 224.5.5.5, the latter in detail mode.

```
console#show ip igmp interface membership 224.5.5.5
               IGMP INTERFACE MEMBERSHIP INFO
Interface  Interface IP       State     Group Compat Source Filter
                                        Mode         Mode
---------  --------------- ----------- ------------ -------------
```

```
console(config)#show ip igmp interface membership 224.5.5.5 detail
                IGMP INTERFACE DETAILED MEMBERSHIP INFO
Interface  Group Compat  Source Filter  Source Hosts   Expiry Time
           Mode          Mode
---------- ------------- -------------- -------------- ------------
```

show ip igmp interface stats

Use the **show ip igmp interface stats** command in User EXEC mode to display the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Syntax

show ip igmp interface stats vlan *vlan-id*

- *vlan-id*—Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Examples

The following example displays the IGMP statistical information for VLAN 7.

```
console#show ip igmp interface stats vlan 7
Querier Status.............................. Querier
Querier IP Address.......................... 7.7.7.7
Querier Up Time (secs) ..................... 55372
Querier Expiry Time (secs) ................. 0
Wrong Version Queries....................... 0
Number of Joins............................. 7
Number of Groups............................ 1
```

ip igmp router-alert-optional

Use the **ip igmp router-alert-optional** command to set IGMP to not require the Router-Alert field.

Syntax

ip igmp router-alert-optional

no ip igmp router-alert-optional

Default Value

The Router-Alert field is not required by default.

Command Mode

Global Configuration

Usage Guidelines

No specific guidelines

Example

```
ip igmp router-alert-optional
```

45

IGMP Proxy Commands

ip igmp-proxy

Use the **ip igmp-proxy** command in Interface Configuration mode to enable the IGMP Proxy on the router. To enable the IGMP Proxy on the router, multicast forwarding must be enabled and there must be no multicast routing protocols enabled on the router.

Syntax

ip igmp-proxy

no ip igmp-proxy

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the IGMP Proxy on the VLAN 15 router.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy
```

ip igmp-proxy reset-status

Use the **ip igmp-proxy reset-status** command in Interface Configuration mode to reset the host interface status parameters of the IGMP Proxy router. This command is valid only when IGMP Proxy is enabled on the interface.

Syntax

ip igmp-proxy reset-status

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example resets the host interface status parameters of the IGMP Proxy router.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp-proxy reset-status
```

ip igmp-proxy unsolicited-report-interval

Use the **ip igmp-proxy unsolicited-report-interval** command in Interface Configuration mode to set the unsolicited report interval for the IGMP Proxy router. This command is valid only if IGMP Proxy on the interface is enabled.

Syntax

ip igmp-proxy unsolicited-report-interval *seconds*

- *seconds*—Unsolicited report interval. (Range: 1-260 seconds)

Default Configuration

The default configuration is 1 second.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets 10 seconds as the unsolicited report interval for the IGMP Proxy router.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip igmp-proxy unsolicited-report-
interval 10
```

show ip igmp-proxy

Use the **show ip igmp-proxy** command in Privileged EXEC mode to display a summary of the host interface status parameters. It displays status parameters only when IGMP Proxy is enabled.

Syntax

show ip igmp-proxy

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of the host interface status parameters.

```
console#show ip igmp-proxy

Interface Index.............................. vlan13

Admin Mode.................................... Enable

Operational Mode.............................. Enable

Version....................................... 3

Number of Multicast Groups.................... 0

Unsolicited Report Interval................... 1

Querier IP Address on Proxy Interface......... 0.0.0.0

Older Version 1 Querier Timeout............... 0

Older Version 2 Querier Timeout............... 0

Proxy Start Frequency......................... 1
```

show ip igmp-proxy interface

Use the **show ip igmp-proxy interface** command in Privileged EXEC mode to display a detailed list of the host interface status parameters. It displays status parameters only when IGMP Proxy is enabled.

Syntax

show ip igmp-proxy interface

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example fails to display status parameters because IGMP Proxy is not enabled.

```
console#show ip igmp-proxy interface

Interface Index.............................. vlan13
```

```
Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----------------------------------------------------------------
1          0            0            0        -----       -----
2          0            0            0            0           0
3          0            0            0        -----       -----
```

show ip igmp-proxy groups

Use the **show ip igmp-proxy groups** command in Privileged EXEC mode to display a table of information about multicast groups that IGMP Proxy reported. It displays status parameters only when IGMP Proxy is enabled.

Syntax

show ip igmp-proxy groups

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example attempts to display a table of information about multicast groups that IGMP Proxy reported.

```
console#show ip igmp-proxy groups
Interface Index.............................. vlan13
Group Address  Last Reporter    Up Time   Member State Filter Mode Sources
-------------  ---------------  -------   ------------ ----------- -------
225.0.1.1        13.13.13.1    7         DELAY-MEMBER Exclude      0
225.0.1.2        13.13.13.1    48        DELAY-MEMBER Exclude      0
```

show ip igmp-proxy groups detail

Use the **show ip igmp-proxy groups detail** command in Privileged EXEC mode to display complete information about multicast groups that IGMP Proxy has reported.

Syntax

show ip igmp-proxy groups detail

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays complete information about multicast groups that IGMP Proxy has reported.

```
console#show ip igmp-proxy groups detail

Interface Index.............................. vlan13
Group Address  Last Reporter    Up Time   Member State Filter Mode Sources
-------------  ---------------  -------   ------------ ----------- -------
225.0.1.1        13.13.13.1       26     DELAY-MEMBER Exclude      0
225.0.1.2        13.13.13.1       67     DELAY-MEMBER Exclude      0
```

46

IP Routing Commands

encapsulation

Use the **encapsulation** command in Interface Configuration mode to configure the link layer encapsulation type for the packet. Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

Syntax

encapsulation {**ethernet** | **snap**}

- **ethernet**—Specifies Ethernet encapsulation.
- **snap**—Specifies SNAP encapsulation.

Default Configuration

Ethernet encapsulation is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example applies SNAP encapsulation for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#encapsulation snap
```

ip address

Use the **ip address** command in Interface Configuration mode to configure an IP address on an interface. Also use this command to configure one or more secondary IP addresses on the interface. This command changes the label IP address in the show IP interface.

Syntax

ip address *ip-address* {*subnet-mask* | *prefix-length*} [**secondary**]

no ip address *ip-address* {*subnet-mask* | *prefix-length*} [**secondary**]

- *ip-address*—IP address of the interface.
- *subnet-mask*—Subnet mask of the interface
- *prefix-length*—Length of the prefix. Must be preceded by a forward slash (/). (Range: 1-30 bits)
- **secondary**—Indicates the IP address is a secondary address.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Loopback) mode

User Guidelines

This command also implicitly enables the interface for routing (i.e. as if the user had issued the 'routing' interface command).

Example

The following example defines the IP address and subnet mask for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip address 192.168.10.10 255.255.255.0
```

ip mtu

Use the **ip mtu** command in Interface Configuration mode to set the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Use the no form of the command to return the MTU size to the default value.

Software currently does not fragment IP packets. Packets forwarded in hardware ignore the IP MTU. Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface. Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the **ip mtu** command. OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency (unless OSPF has been instructed to ignore differences in IP MTU with the **ip ospf mtuignore** command).

Syntax

ip mtu *integer*

- *integer*—Specifies the distance (preference) of an individual static route. (Range: 68-1500)

Default Configuration

1500 bytes is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example defines 1480 as the MTU for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip mtu 1480
```

ip netdirbcast

Use the **ip netdirbcast** command in Interface Configuration mode to enable the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped. Use the no form of the command to disable the broadcasts.

Syntax

ip netdirbcast

no ip netdirbcast

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example defines the IP address and subnet mask for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip netdirbcast
```

ip route

Use the **ip route** command in Global Configuration mode to configure a static route. Use the no form of the command to delete the static route. The IP route command sets a value for the route preference. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. Specifying the preference of a static route controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

Syntax

ip route *ip-address* {*subnet-mask* | *prefix-length*} *next-hop-ip* [**metric** *preference*]

no ip route *ip-address subnet-mask* [*next-hop-ip*] [**metric** *preference*]

- *ip-address*—IP address of destination interface.
- *subnet-mask*—Subnet mask of destination interface.
- *prefix-length*—Length of prefix. Must be preceded with a forward slash (/). (Range: 0-32 bits)
- *next-hop-ip*—IP address of the next hop router.
- *preference*—Specifies the preference value, a.k.a. administrative distance, of an individual static route. (Range: 1-255)

Default Configuration

Default value of preference is 1.

Command Mode

Global Configuration mode

User Guidelines

For the static routes to be visible, you must:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Example

The following example identifies the *ip-address subnet-mask*, *next-hop-ip* and a preference value of 200.

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1
metric 200
```

ip route default

Use the **ip route default** command in Global Configuration mode to configure the default route. Use the no form of the command to delete the default route.

Syntax

ip route default [*next-hop-ip*] [*preference*]

no ip route default [*next-hop-ip* [*preference*]

- *next-hop-ip*—IP address of the next hop router.
- *preference*—Specifies the preference value, a.k.a administrative distance, of an individual static route. (Range: 1-255)

Default Configuration

Default value of preference is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example identifies the *next-hop-ip* and a preference value of 200.

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1
200
```

ip route distance

Use the **ip route distance** command in Global Configuration mode to set the default distance (preference) for static routes. Lower route preference values are preferred when determining the best route. The **ip route** and **ip route default** commands allow optional setting of the distance of an individual static route. The default distance is used when no distance is specified in these

commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance are applied to static routes created after invoking the **ip route distance** command.

Syntax

ip route distance *integer*

no ip route distance *integer*

- *integer*—Specifies the distance (preference) of an individual static route. (Range 1-255)

Default Configuration

Default value of distance is 1.

Command Mode

Global Configuration mode

User Guidelines

Lower route distance values are preferred when determining the best route.

Example

The following example sets the default route metric to 80.

```
console(config)#ip route distance 80
```

ip routing

To globally enable IPv4 routing on the router, use the "ip routing" command in Global Configuration mode. To disable IPv4 routing globally, use the **no** form of this command.

Syntax

ip routing

no ip routing

Default Configuration

The ip routing default configuration is disabled.

Command Mode

Global Config

User Guidelines

Use this command to globally enable IPv4 routing.

Example

```
console(config)#ip routing
```

routing

Use the **routing** command in Interface Configuration mode to enable IPv4 and IPv6 routing for an interface. View the current value for this function with the **show ip brief** command. The value is labeled Routing Mode in the output display. Use the no form of the command to disable routing for an interface.

Syntax

routing

no routing

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IPv4 and IPv6 routing for VLAN 15

```
console(config)#interface vlan 15
console(config-if-vlan15)#routing
```

show ip brief

Use the **show ip brief** command in Privileged EXEC mode to display all the summary information of the IP.

Syntax

show ip brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IP summary information.

```
console#show ip brief

Default Time to Live.......................... 30

Routing Mode.................................. Disabled

IP Forwarding Mode............................ Enabled

Maximum Next Hops............................. 2
```

show ip interface

Use the **show ip interface** command in Privileged EXEC mode to display all pertinent information about one or more IP interfaces.

Syntax

show ip interface [**vlan** *vlan-id* | **loopback** *loopback -id*]

- *vlan-id*—Valid VLAN ID
- *loopback-id*—Valid loopback ID. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display all IP information and information specific to VLAN 15.

```
console#show ip interface

Management Interface:

IP Address.................................... 10.240.4.125

Subnet Mask................................... 255.255.255.0

Default Gateway............................... 10.240.4.1
```

```
Burned In MAC Address..................... 00:10:18:82:04:35
Network Configuration Protocol Current..... None
Management VLAN ID........................ 1
Routing Interfaces:
Netdir Multi
Interface  IP Address      IP Mask          Bcast   CastFwd
---------- --------------- --------------- -------- --------
vlan1      192.168.10.10   255.255.255.0   Disable  Disable
vlan2      0.0.0.0         0.0.0.0         Enable   Disable
loopback2  0.0.0.0         0.0.0.0         Disable  Disable

console#show ip interface vlan 15
Primary IP Address.........................
192.168.10.10/255.255.255.0
Secondary IP Address(es)...................
192.168.20.20/255.255.255.0
Routing Mode.............................. Disable
Administrative Mode....................... Disable
Forward Net Directed Broadcasts........... Disable
Proxy ARP................................. Enable
Local Proxy ARP........................... Disable
Active State.............................. Inactive
Link Speed Data Rate...................... Inactive
MAC Address............................... 00:00:00:01:00:02
Encapsulation Type........................ Ethernet
IP MTU.................................... 1500
```

show ip protocols

Use the **show ip protocols** command in Privileged EXEC mode to display the parameters and current state of the active routing protocols.

Syntax

show ip protocols

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays parameters and current state of active routing protocols.

```
console#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds
Invalid after 180 seconds, hold down 120, flushed after 300
Redistributing: RIP, Static, OSPF
Default version control: send version 1, receive version 1
Interfaces:
Interface Send Receive Key-chain
176.1.1.1 1 1 flowers
176.2.1.1 passive 2
Routing Information Sources:
Gateway Last Update
176.1.1.2 0:00:17
Preference: 60
Routing Protocol is "ospf"
Redistributing: OSPF, External direct, Static, RIP
Interfaces:
Interface Metric Key-chain
176.1.1.1 10 flowers
```

```
176.2.1.1 1

Routing Information Sources:

Gateway State

176.1.1.2 Full

External Preference: 60

Internal Preference: 20
```

show ip route

Use the **show ip route** command in Privileged EXEC mode to display the routing table.

Syntax

show ip route [*protocol* | **address** *ip-address* [*subnet-mask* | *prefix-length*] [**longer-prefixes**]]

- *protocol*—Specifies the protocol that installed the routes. (Range: connected, ospf, rip static)
- *ip-address*—Specifies the network for which the route is to be displayed and displays the best matching best-route for the address.
- *subnet-mask*—Subnet mask of the IP address.
- *prefix-length*—Length of prefix, in bits. Must be preceded with a forward slash ('/'). (Range: 0-32 bits)
- **longer-prefixes**—Indicates that the *ip-address* and *subnet-mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the routing table.

```
console#show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S -
Static
```

```
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA external type 2
```

show ip route preferences

Use the **show ip route preferences** command in Privileged EXEC mode displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Syntax

show ip route preferences

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IP route preferences.

```
console#show ip route preferences
Local.......................................... 0
Static......................................... 1
OSPF Intra..................................... 8
OSPF Inter..................................... 10
OSPF Ext T1.................................... 13
OSPF Ext T2.................................... 150
OSPF NSSA T1................................... 14
OSPF NSSA T2................................... 151
RIP............................................ 15
```

show ip route summary

Use the **show ip route summary** command in Privileged EXEC mode to display the routing table summary.

Syntax

show ip route summary [**all**]

- **all**—Shows the number of all routes, including best and non-best routes. To include only the number of best routes, do not use this optional parameter.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the IP route summary.

```
console#show ip route summary

Connected Routes.............................. 0

Static Routes................................. 0

RIP Routes.................................... 0

OSPF Routes................................... 0

Intra Area Routes............................. 0

Inter Area Routes............................. 0

External Type-1 Routes........................ 0

External Type-2 Routes........................ 0

Total routes.................................. 0
```

show ip stats

Use the **show ip stats** command in User EXEC mode to display IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Syntax

show ip stats

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IP route preferences.

```
console>show ip stats

IpInReceives..................................... 24002

IpInHdrErrors.................................... 1

IpInAddrErrors................................... 925

IpForwDatagrams.................................. 0

IpInUnknownProtos................................ 0

IpInDiscards..................................... 0

IpInDelivers..................................... 18467

IpOutRequests.................................... 295

IpOutDiscards.................................... 0

IpOutNoRoutes.................................... 0

IpReasmTimeout................................... 0

IpReasmReqds..................................... 0

IpReasmOKs....................................... 0

IpReasmFails..................................... 0

IpFragOKs........................................ 0

IpFragFails...................................... 0

IpFragCreates.................................... 0

IpRoutingDiscards................................ 0
```

```
IcmpInMsgs..................................... 3
IcmpInErrors................................... 0
IcmpInDestUnreachs............................. 0
IcmpInTimeExcds................................ 0
IcmpInParmProbs................................ 0
IcmpInSrcQuenchs............................... 0
IcmpInRedirects................................ 0
IcmpInEchos.................................... 3
IcmpInEchoReps................................. 0
IcmpInTimestamps............................... 0
IcmpInTimestampReps............................ 0
IcmpInAddrMasks................................ 0
IcmpInAddrMaskReps............................. 0
IcmpOutMsgs.................................... 3
IcmpOutErrors.................................. 0
IcmpOutDestUnreachs............................ 0
IcmpOutTimeExcds............................... 0
IcmpOutParmProbs............................... 0
IcmpOutSrcQuenchs.............................. 0
IcmpOutRedirects............................... 0
IcmpOutEchoReps................................ 3
IcmpOutTimestamps.............................. 0
IcmpOutTimestampReps........................... 0
IcmpOutAddrMasks............................... 0
```

47

IPv6 Routing Commands

clear ipv6 neighbors

Use the **clear ipv6 neighbors** command in Privileged EXEC mode to clear all entries in the IPv6 neighbor table or an entry on a specific interface.

Syntax

clear ipv6 neighbors [**vlan** *vlan-id*]

- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears all entries in the IPv6 neighbor table.

```
console(config)#clear ipv6 neighbors
```

clear ipv6 statistics

Use the **clear ipv6 statistics** command in Privileged EXEC mode to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces. IPv6 statistics display in the output of the **show ipv6 traffic** command.

Syntax

clear ipv6 statistics [**vlan** *vlan-id*| **tunnel** *tunnel-id* | **loopback** *loopback-id*]

- *vlan-id*—Valid VLAN ID.
- *tunnel-id*—Tunnel identifier. (Range: 0-7)
- *loopback-id*—Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears IPv6 statistics for VLAN 11.

```
console(config)#clear ipv6 statistics vlan 11
```

ipv6 address

Use the **ipv6 address** command in Interface Configuration mode to configure an IPv6 address on an interface (including tunnel and loopback interfaces) and to enable IPv6 processing on this interface. Multiple globally reachable addresses can be assigned to an interface by using this command. There is no need to assign a link-local address by using this command since one is automatically created. IPv6 addresses can be expressed in eight blocks. Also of note is that instead of a period, a colon separates each block. For simplification, leading zeros of each 16-bit block can be omitted. One sequence of 16-bit blocks containing only zeros can be replaced with a double colon "::", but not more than one at a time (otherwise it is no longer a unique representation).

Dropping zeros: 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1

Local host: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1

Any host: 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is 3ffe:1::1234/64.

Syntax

ipv6 address *prefix/prefix-length* [**eui64**]

no ipv6 address [*prefix/prefix-length*] [**eui64**]

- *prefix*—Consists of the bits of the address to be configured.

- *prefix-length*—Designates how many of the high-order contiguous bits of the address make up the prefix.
- **eui64**—The optional **eui-64** field designates that IPv6 processing on the interfaces is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If this option is used, the value of *prefix_length* must be 64 bits.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an IPv6 address and enables IPv6 processing.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 address 2020:1::1/64
```

ipv6 enable

Use the **ipv6 enable** command in Interface Configuration mode to enable IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address. Command execution automatically configures the interface with a link-local address. The command is not required if an IPv6 global address is configured on the interface.

Syntax

ipv6 enable

no ipv6 enable

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IPv6 routing, which has not been configured with an explicit IPv6 address.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 enable
```

ipv6 forwarding

Use the **ipv6 forwarding** command in Global Configuration mode to enable IPv6 forwarding on a router.

Syntax

ipv6 forwarding

no ipv6 forwarding

Default Configuration

Enabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables IPv6 forwarding.

```
console#configure
console(config)#ipv6 forwarding
console(config)#no ipv6 forwarding
```

ipv6 mtu

Use the **ipv6 mtu** command in Interface Configuration mode to set the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface. This command replaces the default or link MTU with a new MTU value.

Syntax

ipv6 mtu *mtu*

no ipv6 mtu

- *mtu*—Is the maximum transmission unit. (Range: 1280-1500)

Default Configuration

The default MTU is 1500.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 mtu 1300
```

ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** command in Interface Configuration mode to set the number of duplicate address detection probes transmitted while doing neighbor discovery. Duplicate address detection verifies that an IPv6 address on an interface is unique.

Syntax

ipv6 nd dad attempts *attempts*

no ipv6 nd dad attempts

- *attempts*—Probes transmitted. (Range: 0-600)

Default Configuration

1 is the default value for attempts.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets at 10 the number of duplicate address detection probes transmitted while doing neighbor discovery.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd dad attempts 10
```

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command in Interface Configuration mode to set the "managed address configuration" flag in router advertisements. When the value is true,

end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Syntax

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Default Configuration

False is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

In the following example, the end node uses DHCPv6.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

Use the **ipv6 nd ns-interval** command in Interface Configuration mode to set the interval between router advertisements for advertised neighbor solicitations. An advertised value of 0 means the interval is unspecified.

Syntax

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

- *milliseconds*—Interval duration. (Range: 0, 1000 - 4294967295)

Default Configuration

0 is the default value for *milliseconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the interval between router advertisements for advertised neighbor solicitations at 5000 ms.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 nd ns-interval 5000
```

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command in Interface Configuration mode to set the "other stateful configuration" flag in router advertisements sent from the interface.

Syntax

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Default Configuration

False is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets to true the "other stateful configuration" flag in router advertisements

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd other-config-flag
```

ipv6 nd prefix

Use the **ipv6 nd prefix** command to configure parameters associated with prefixes that the router advertises in its router advertisements.

Syntax

ipv6 nd prefix *prefix/prefix-length* [{*valid-lifetime*| **infinite**} {*preferred-lifetime*| **infinite**}] [**noautoconfig**] [**off-link**]

no ipv6 nd prefix *prefix/prefix-length*

- *prefix*—IPv6 prefix.
- *prefix-length*—IPv6 prefix length.
- *valid-lifetime*—Valid lifetime of the router in seconds. (Range: 0-4294967295 seconds)
- **infinite**—Indicates lifetime value is infinite.
- *preferred-lifetime*—Preferred-lifetime of the router in seconds. (Range: 0-4294967295 seconds)
- **no-autocoding**—Do not use Prefix for autoconfiguration.
- **off-link**—Do not use Prefix for onlink determination.

Default Configuration

604800 seconds is the default value for valid-lifetime, 2592000 seconds for preferred lifetime.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the ipv6 address interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the **ipv6 nd prefix** command to configure these values.

The ipv6 nd prefix command will allow you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the **ipv6 address** command. Prefixes specified using ipv6 nd prefix without an associated interface address will not be included in RAs and will not be committed to the device configuration.

Example

The following example sets the IPv6 prefixes to include in the router advertisement.

```
console(config)#interface vlan 11
console(config-if-vlan11)#ipv6 nd prefix 2020:1::1/64
```

ipv6 nd ra-interval

Use the **ipv6 nd ra-interval** command in Interface Configuration mode to set the transmission interval between router advertisements.

Syntax

ipv6 nd ra-interval *seconds*

no ipv6 nd ra-interval

- *seconds*—Interval duration. (Range: 4-1800)

Default Configuration

600 is the default value for *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the transmission interval between router advertisements at 1000 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ra-interval 1000
```

ipv6 nd ra-lifetime

Use the **ipv6 nd ra-lifetime** command in Interface Configuration mode to set the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.

Syntax

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

- *seconds*—Lifetime duration. The value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000 seconds. A value of zero means this router is not to be used as the default router. (Range: 0-9000)

Default Configuration

1800 is the default value for *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets at 1000 seconds the value that is placed in the Router Lifetime field of the router advertisements.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 nd ra-lifetime 1000
```

ipv6 nd reachable-time

Use the **ipv6 nd reachable-time** command in Interface Configuration mode to set the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.

Syntax

ipv6 nd reachable-time milli*seconds*

no ipv6 nd reachable-time

- *milliseconds*—Reachable-time duration. A value of zero means the time is unspecified by the router. (Range: 0-3600000 milliseconds)

Default Configuration

The default value for neighbor discovery reachable times is 0 milliseconds.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the router advertisement time at 5000 milliseconds to consider a neighbor reachable after neighbor discovery confirmation.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 nd reachable-time 5000
```

ipv6 nd suppress-ra

Use the **ipv6 nd suppress-ra** command in Interface Configuration mode to suppress router advertisement transmission on an interface.

Syntax

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example suppresses router advertisement transmission.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 nd suppress-ra
```

ipv6 route

Use the **ipv6 route** command in Global Configuration mode to configure an IPv6 static route.

Syntax

ipv6 route *ipv6-prefix /prefix-length* [**interface** {**tunnel** *tunnel-id* | **vlan** ***vlan-id***}]*next-hop-address preference*

no ipv6 route *ipv6-prefix /prefix-length* [**interface** {**tunnel** ***tunnel-id*** | **vlan** ***vlan-id***}]*next-hop-address preference*

- *ipv6-prefix*—Is the IPv6 network that is the destination of the static route.
- *prefix-length*—Is the length of the IPv6 prefix — a decimal value (usually 0-64) that shows 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 it.
- **interface**—Identifies direct static routes from point-to-point and broadcast interfaces, and must be specified when using a link-local address as the next hop.
- **tunnel or vlan**—Is the tunnel or vlan interface to associate with the route.
- *next-hop-address*—Is the IPv6 address of the next hop that can be used to reach the specified network.
- *preference*—Is a value the router uses to compare this route with routes from other route sources that have the same destination. (Range: 1-255)

Default Configuration

1 is the default value for *preference*.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configure an IPv6 static route.

```
console(config)#ipv6 route 2020:1::1/64 2030:1::2
```

ipv6 route distance

Use the **ipv6 route distance** command in Global Configuration mode to set the default distance (preference) for static routes. Lower route preference values are preferred when determining the best route. The **ipv6 route** and **ipv6 route default** commands allow optional setting of the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance is applied to static routes created after invoking the **ipv6 route distance** command.

Syntax

ipv6 route distance *integer*

no ipv6 route distance *integer*

- *integer*—Specifies the distance (preference) of an individual static route. (Range 1-255)

Default Configuration

Default value of *integer* is 1.

Command Mode

Global Configuration mode

User Guidelines

Lower route distance values are preferred when determining the best route.

Example

The following example sets the default distance to 80.

```
console(config)#ipv6 route distance 80
```

ipv6 unicast-routing

Use the **ipv6 unicast-routing** command in Global Configuration mode to enable forwarding of IPv6 unicast datagrams.

Syntax

ipv6 unicast-routing

no ipv6 unicast-routing

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables Ipv6 unicast datagram forwarding.

```
console(config)#ipv6 unicast-routing
```

```
console(config)#no ipv6 unicast-routing
```

ping ipv6

Use ping ipv6 command in Privileged EXEC mode to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Syntax

ping ipv6 *ipv6-address* [**size** *size*]

- *ipv6-address*—Target IPv6 address to ping.
- *size*—Size of the datagram. (Range: 48-2048 bytes)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example determines whether another computer is on the network at the IPv6 address specified.

```
console(config)#ping ipv6 2030:1::1/64

Send count=3, Receive count=0 from 2030:1::1/64

Average round trip time = 0.00 ms
```

ping ipv6 interface

Use **ping ipv6 interface** command in the Privileged EXEC mode to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the

workstation. The terminal interface sends three pings to the target station. Use the **interface** keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. The source can be a loopback, tunnel, or logical interface.

Syntax

ping ipv6 interface {**vlan** *vlan-id*| **tunnel** *tunnel-id*} | **loopback** *loopback-id*} *link-local-address* [**size** *datagram-size*]

- *vlan-id*—Valid VLAN ID.
- *tunnel-id*—Tunnel identifier. (Range: 0-7)
- *loopback-id*—Loopback identifier. (Range: 0-7)
- *link-local-address*—IPv6 address to ping.
- *datagram-size*—Size of the datagram. (Range: 48-2048 bytes)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example determines whether another computer is on the network at the IPv6 address specified.

```
console(config)#ping ipv6 interface loopback 1
FE80::202:BCFF:FE00:3068/128

Send count=3, Receive count=0 from FE80::202:BCFF:FE00:3068/128

Average round trip time = 0.00 ms
```

show ipv6 brief

Use the **show ipv6 brief** command in Privileged EXEC mode to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Syntax

show ipv6 brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.

```
console#show ipv6 brief

IPv6 Forwarding Mode.......................... Enable

IPv6 Unicast Routing Mode..................... Disable

IPv6 Hop Limit.................................1
```

show ipv6 interface

Use the **show ipv6 interface** command in Privileged EXEC mode to show the usability status of IPv6 interfaces.

Syntax

show ipv6 interface {**brief**|**loopback** *loopback-id*| **tunnel** *tunnel-id*|**vlan** *vlan-id*}

- *loopback-id*—Valid loopback interface ID
- *tunnel-id*—Valid tunnel interface ID
- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples show the usability status of a IPv6 VLAN interface individually and all IPv6 interfaces collectively in an abbreviated format.

```
console#show ipv6 interface vlan 3
```

```
IPv6 is enabled
IPv6 Prefix is ..................... FE80::2FC:E3FF:FE90:147/128
                                     3FF0:1236:C261::1/64
Routing Mode.................................. Enabled
Administrative Mode........................... Enabled
IPv6 Routing Operational Mode................. Enabled
Interface Maximum Transmit Unit............... 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval.............. 0
Router Lifetime Interval...................... 1800
Router Advertisement Reachable Time........... 0
Router Advertisement Interval................. 600
Router Advertisement Managed Config Flag...... Disabled
Router Advertisement Other Config Flag........ Disabled
Router Advertisement Suppress Flag............ Disabled

Prefix 3FF0:1236:C261::1/64
Preferred Lifetime............................ 10000
Valid Lifetime................................ 100000
Onlink Flag................................... Enabled
Autonomous Flag............................... Enabled

console#show ipv6 interface brief
           Oper.
Interface  Mode      IPv6 Address/Length
---------- -------- ---------------------------------
vlan3      Enabled  FE80::2FC:E3FF:FE90:147/128
                    3FF0:1236:C261::1/64
loopback 1 Enabled  FE80::2FC:E3FF:FE90:145/128
                    3FF0:C221:1234::1/64
```

```
loopback 2 Disabled
tunnel 1   Disabled 3FFE:1234::1/64                          [TENT]
```

show ipv6 neighbors

Use the **show ipv6 neighbors** command in Privileged EXEC mode to display information about the IPv6 neighbors.

Syntax

show ipv6 neighbors

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the IPv6 neighbors.

```
console(config)#show ipv6 neighbors
Neighbor Last
IPv6 Address         MAC Address       isRtr  State   Updated
                                                       Interface
-------------------- ----------------- -----  ------- ---------
```

show ipv6 route

Use the **show ipv6 route** command in Privileged EXEC mode to display the IPv6 routing table.

Syntax

show ipv6 route [{*ipv6-address* [*protocol*] | {{*ipv6-prefix*/ *ipv6-prefix-length* | *interface*} [*protocol*] | *protocol* [**all**] | **all**}]

- *ipv6-address*—Specifies an IPv6 address for which the best-matching route would be displayed.

- *protocol*—Specifies the protocol that installed the routes. Is one of the following keywords: connected, ospf, static.
- *ipv6-prefix/ipv6 prefix-length*—Specifies a IPv6 network for which the matching route would be displayed.
- *interface*—Valid IPv6 interface. Specifies that the routes with next-hops on the selected interface be displayed.
- **all**—Specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed. If the connected keyword is selected for protocol, the **all** option is not available because there are no best or non-best connected routes.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the IPv6 routing table.

```
console(config)#show ipv6 route

IPv6 Routing Table - 0 entries

Codes: C - connected, S - static

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2

ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
```

show ipv6 route preferences

Use the **show ipv6 route preferences** command in Privileged EXEC mode to show the preference value associated with the type of route. Lower numbers have a greater preference.

Syntax

show ipv6 route preferences

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows the preference value associated with the type of route.

```
console#show ipv6 route preferences

Local..................................... 0

Static.................................... 1

OSPF Intra................................ 8

OSPF Inter................................ 10

OSPF Ext T1............................... 13

OSPF Ext T2............................... 150

OSPF NSSA T1.............................. 14

OSPF NSSA T2.............................. 151
```

show ipv6 route summary

Use the **show ipv6 route summary** command in Privileged EXEC mode to display a summary of the routing table. Use **all** to display the count summary for all routes, including best and non-best routes. Use the command without parameters to display the count summary for only the best routes.

Syntax

show ipv6 route summary [**all**]

- **all**—Displays the count summary for all routes.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of the routing table.

```
console#show ipv6 route summary

IPv6 Routing Table Summary - 0 entries

Connected Routes.............................. 0

Static Routes................................. 0

OSPF Routes................................... 0

Intra Area Routes............................. 0

Inter Area Routes............................. 0

External Type-1 Routes........................ 0

External Type-2 Routes........................ 0

Total routes.................................. 0

Number of Prefixes:
```

show ipv6 traffic

Use the **show ipv6 traffic** command in User EXEC mode to show traffic and statistics for IPv6 and ICMPv6.

Syntax

show ipv6 traffic [**vlan** *vlan-id* | **tunnel** *tunnel-id* | **loopback** *loopback-id*]

- *vlan-id*—Valid VLAN ID, shows information about traffic on a specific interface or, without the optional parameter, shows information about traffic on all interfaces.
- **tunnel**—Tunnel identifier. (Range: 0-7)
- **loopback**—Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples show traffic and statistics for IPv6 and ICMPv6, first for all interfaces and an individual VLAN.

```
console> show ipv6 traffic

IPv6 STATISTICS

Total Datagrams Received..............................  0

Received Datagrams Locally Delivered..................  0

Received Datagrams Discarded Due To Header Errors.....  0

Received Datagrams Discarded Due To MTU...............  0

Received Datagrams Discarded Due To No Route..........  0

Received Datagrams With Unknown Protocol..............  0

Received Datagrams Discarded Due To Invalid Address...  0

Received Datagrams Discarded Due To Truncated Data....  0

Received Datagrams Discarded Other....................  0

Received Datagrams Reassembly Required................  0

Datagrams Successfully Reassembled....................  0

Datagrams Failed To Reassemble........................  0

Datagrams Forwarded...................................  0

Datagrams Locally Transmitted.........................  0

Datagrams Transmit Failed.............................  0

Datagrams Successfully Fragmented.....................  0

Datagrams Failed To Fragment..........................  0

Fragments Created.....................................  0

Multicast Datagrams Received..........................  0

Multicast Datagrams Transmitted.......................  0


console> show ipv6 traffic vlan 11

Interface ..............................  11

IPv6 STATISTICS

Total Datagrams Received..............................  0
```

```
Received Datagrams Locally Delivered..................... 0
Received Datagrams Discarded Due To Header Errors........ 0
Received Datagrams Discarded Due To MTU.................. 0
Received Datagrams Discarded Due To No Route............. 0
Received Datagrams With Unknown Protocol................. 0
Received Datagrams Discarded Due To Invalid Address...... 0
Received Datagrams Discarded Due To Truncated Data........ 0
Received Datagrams Discarded Other....................... 0
Received Datagrams Reassembly Required................... 0
Datagrams Successfully Reassembled....................... 0
Datagrams Failed To Reassemble........................... 0
Datagrams Forwarded...................................... 0
Datagrams Locally Transmitted............................ 0
Datagrams Transmit Failed................................ 0
Datagrams Successfully Fragmented........................ 0
Datagrams Failed To Fragment............................. 0
Fragments Created........................................ 0
Multicast Datagrams Received............................. 0
Multicast Datagrams Transmitted.......................... 0
```

show ipv6 vlan

Use the **show ipv6 vlan** command in Privileged EXEC mode to display IPv6 VLAN routing interface addresses.

Syntax

show ipv6 vlan

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IPv6 VLAN routing interface addresses.

```
console#show ipv6 vlan
MAC Address used by Routing VLANs: 00:02:BC:00:30:68
VLAN ID IPv6 Address/Prefix Length
------- ------------------------------------
1
```

traceroute ipv6

Use the **traceroute ipv6** command in Privileged EXEC mode to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

Syntax

traceroute ipv6 *ipv6-address* [*port*]

- *ipv6-address*—Destination IPv6 address.
- *port*—UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. (Range: 0-65535)

Default Configuration

33434 is the default port value.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example discovers the packet routes on a hop-by-hop basis.

```
console#traceroute ipv6 2020:1::1

Tracing route over a maximum of 20 hops

1 * N * N * N
```

48

Loopback Interface Commands

interface loopback

Use the **interface loopback** command in Global Configuration mode to enter the Interface Loopback configuration mode.

Syntax

interface loopback *loopback-id*

no interface loopback *loopback-id*

- *loopback-id*—Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the Interface Loopback 1 configuration mode.

```
console(config)# interface loopback 1
console(config-if-loopback1)#
```

show interfaces loopback

Use the **show interfaces loopback** command in Privileged EXEC mode to display information about one or all configured loopback interfaces.

Syntax

show interfaces loopback [*loopback-id*]

- *loopback-id*—Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display information about configured loopback interfaces.

```
console# show interfaces loopback
Loopback Id  Interface  IP Address Received Packets Sent Packets
------------ ---------- ---------- ---------------- -------------
1            loopback 1 0.0.0.0    0                0

console# show interfaces loopback 1
Interface Link Status..........................  Up
IP Address..................................... 0.0.0.0 0.0.0.0
MTU size....................................... 1500 bytes
```

49

Multicast Commands

ip mcast boundary

Use the **ip mcast boundary** command in Interface Configuration mode to add an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable. *groupipaddr* is a group IP address and *mask* is a group IP mask.

Syntax

ip mcast boundary *groupipaddr mask*

no ip mcast boundary *groupipaddr mask*

- *groupipaddr*—IP address of multicast group. Valid range is 239.0.0.0 to 239.255.255.255.
- *mask*—IP mask of multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example adds an administrative scope multicast boundary.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip mcast boundary 239.5.5.5
255.255.255.255
```

ip multicast

Use the **ip multicast** command in Global Configuration mode to set the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message is displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Syntax

ip multicast

no ip multicast

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IP multicast on the router.

```
console#configure


console(config)#ip multicast
console(config)#no ip multicast
```

ip multicast staticroute

Use the **ip multicast staticroute** command in Global Configuration mode to create a static route which is used to perform RPF checking in multicast packet forwarding. The combination of the *sourceipaddr* and the *mask* fields specify the network IP address of the multicast packet source. The *rpfipaddr* is the IP address of the next hop toward the source. *metric* is the cost of the route entry for comparison with other routes to the source network. The current incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

Syntax

ip multicast staticroute *sourceipaddr mask rpfipaddr metric* **vlan** *vlan-id*

no ip multicast staticroute *sourceipaddr*

- *sourceipaddr*—IP address of multicast packet source.
- *mask*—IP mask of multicast packet source.
- *rpfipaddr*—IP address of next hop toward source.
- *metric*—Cost of route entry. (Range: 0-255)
- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example creates a static route which is used to perform RPF checking in multicast packet forwarding.

```
console(config)#ip multicast staticroute 224.5.5.5 255.255.255.255
10.1.1.1 5 vlan 15
```

ip multicast ttl-threshold

Use the **ip multicast ttl-threshold** command in Interface Configuration mode to apply a *ttlvalue* to a routing interface. *ttlvalue* is the TTL threshold which is applied to the multicast Data packets forwarded through the interface.

Syntax

ip multicast ttl-threshold *ttlvalue*

no ip multicast ttl-threshold *ttlvalue*

- *ttlvalue*—Specifies TTL threshold. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example applies a *ttlvalue* of 5 to the VLAN 15 routing interface.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip multicast ttl-threshold 5
```

mrinfo

Use the **mrinfo** command in Privileged EXEC mode to query the neighbor information for a multicast-capable router specified by *ipaddr*. The default value is the IP address of the system at which the command is issued. The **mrinfo** command can take up to 2 minutes to complete. Only one mrinfo command may be in process at a time. The results of this command will be available in the results buffer pool which can be displayed by using the command **show mrinfo**.

Syntax

mrinfo [*ipaddr*]

- *ipaddr*—IP address of the router.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following queries neighbor information for a multicast-capable router.

```
console(config)#mrinfo 10.1.1.1
```

mstat

Use the **mstat** command in Privileged EXEC mode to find the IP Multicast packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command are available in the results bufferpool, displayed using the command **show mstat**. Bookmark not defined. If a debug command is already in progress, a message is displayed and the new request fails.

Syntax

mstat *source* [*group/receiver*] [*group/receiver*]

- *source*—The IP address of the remote multicast-capable device.
- *group/receiver*—Multicast IP address of the group being displayed/IP address of the receiver device.

Default Configuration

The default value for *group* is 224.2.0.1. The default value for *receiver* is the IP address of the device which issues the command.

Command Mode

Privileged EXEC mode

User Guidelines

Enter the group and receiver IP addresses in any order.

Example

The following example finds the IP Multicast packet rate and loss information path from a source (IP address 10.1.1.1) to a receiver .

```
console(config)#mstat 10.1.1.1
```

mtrace

Use the **mtrace** command in Privileged EXEC mode to find the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command are available in the results buffer pool which can be displayed using the command **show mtrace**.

Syntax

mtrace *sourceipaddr* [*group/destination*] [*group/destination*]

- *sourceipaddr*—The IP address of the remote multicast-capable device.

- *group/destination*—Multicast IP address of the group being displayed/IP address of the receiver device.

Default Configuration

The default value for *group* is 224.2.0.1. The default value for *destination* is the IP address of the device which issues the command.

Command Mode

Privileged EXEC mode

User Guidelines

Enter the group and receiver IP addresses in any order.

Example

The following example finds the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace).

```
console(config)#mtrace 10.1.1.1
```

no ip mcast mroute

Use the **no ip mcast mroute** command in Global Configuration mode to clear entries in the mroute table.

Syntax

no ip mcast mroute {**group** *groupipaddr* | **source** *sourceipaddr* [*groupipaddr*] | **all**}

- *groupipaddr*—Clears the route entries in the mroute table containing the specified multicast group IP addresses.
- *sourceipaddr*—Clears the route entries in the mroute table containing the specified source IP addresses.
- **all**—Clears all entries.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example clears entries in the mroute table.

```
console(config)#no ip mcast mroute all
```

show ip mcast

Use the **show ip mcast** command in Privileged EXEC mode to display the system-wide multicast information.

Syntax

show ip mcast

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide multicast information.

```
console#show ip mcast

Admin Mode..................................... Disable

Protocol State................................. Non-Operational

Table Max Size ................................ 256

Number Of Packets For Which Source Not Found .. 0

Number Of Packets For Which Group Not Found ... 0

Protocol....................................... No Protocol
Enabled

Entry Count ................................... 0

Highest Entry Count ........................... 0
```

show ip mcast boundary

Use the **show ip mcast boundary** command in Privileged EXEC mode to display all the configured administrative scoped multicast boundaries.

Syntax

show ip mcast boundary {**vlan** *vlan-id* | **all**}

- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all the configured administrative scoped multicast boundaries.

```
console#show ip mcast boundary all

MULTICAST BOUNDARY

Interface Group Ip Mask

--------- --------------- ---------------
```

show ip mcast interface

Use the **show ip mcast interface** command in Privileged EXEC mode to display the multicast information for the specified interface.

Syntax

show ip mcast interface {**vlan** *vlan-id* | **all**}

- *vlan-id*—Valid Ethernet port

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast information for VLAN 15.

```
console#show ip mcast interface vlan 15
Interface TTL
--------- -----
```

show ip mcast mroute

Use the **show ip mcast mroute** command in Privileged EXEC mode to display a summary or all the details of the multicast table.

Syntax

show ip mcast mroute {detail | summary}

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary or all the details of the multicast table.

```
console#show ip mcast mroute summary
Multicast Route Table Summary
                                          Incoming  Outgoing
Source IP       Group IP     Protocol     Interface Interface List
--------------- ------------ ---------- --------- ---------------

console#show ip mcast mroute detail
Multicast Route Table
                      Expiry     Up Time
Source Ip Group Ip    Time(secs) (secs)      RPF Neighbor   Flags
--------- ----------- ---------- ----------- --------------- -----
```

show ip mcast mroute group

Use the **show ip mcast mroute group** command in Privileged EXEC mode to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the *groupipaddr* value.

Syntax

show ip mcast mroute group *groupipaddr* {**detail | summary**}

- *groupipaddr*—IP address of the multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces.

```
console#show ip mcast mroute group 224.5.5.5 summary

Multicast Route Table Summary

                                    Incoming  Outgoing

Source IP Group IP        Protocol  Interface Interface List

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


console#show ip mcast mroute group 224.5.5.5 detail

Multicast Route Table

                    Expiry      Up Time

Source Ip Group Ip  Time(secs)  (secs)    RPF Neighbor    Flags

--------- --------- ----------- --------- --------------- -----
```

show ip mcast mroute source

Use the **show ip mcast mroute source** command in Privileged EXEC mode to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the *sourceipaddr* or *sourceipaddr* | *groupipaddr* pair value(s).

Syntax

show ip mcast mroute source *sourceipaddr* {**summary** | *groupipaddr*}

- *sourceipaddr*—IP address of source.
- *groupipaddr*—IP address of multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays multicast configuration settings.

```
console#show ip mcast mroute source 10.1.1.1 summary
Multicast Route Table Summary
                                      Incoming  Outgoing
Source IP  Group IP        Protocol   Interface Interface List
---------- --------------- --------- --------- ----------------


console#show ip mcast mroute source 10.1.1.1 224.5.5.5
Multicast Route Table
                    Expiry     Up Time
Source IP Group IP  Time(secs) (secs)       RPF Neighbor Flags
--------- --------- ---------- ---------- ------------ -----
```

show ip mcast mroute static

Use the **show ip mcast mroute static** command in Privileged EXEC mode to display all the static routes configured in the static mcast table if it is specified or display the static route associated with the particular *sourceipaddr.*

Syntax

show ip mcast mroute static [*sourceipaddr*]

- *sourceipaddr*—IP address of source.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the static routes configured in the static mcast table.

```
console#show ip mcast mroute static

                  STATIC ROUTES

Source IP  Source Mask     RPF Address  Metric Interface

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


console#show ip mcast mroute static 10.1.1.1

Static Route with source IP address 10.1.1.1 does not exist.
```

show mrinfo

Use the **show mrinfo** command in Privileged EXEC mode to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a **mrinfo** command. The results that follow completion of the latest mrinfo are available in the buffer pool after a maximum of two minutes beyond completion of the **show mrinfo** command. A subsequent **mrinfo** command overwrites the contents of the buffer pool with fresh results.

Syntax

show mrinfo

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the static routes configured in the static mcast table.

```
console#show mrinfo

Results for 'show mrinfo'

0.0.0.0 [Flags: ]

Router   Interface   Neighbor  Metric   TTL Flags

-------- ---------   ------    ------   ----------
```

show mstat

Use the **show mstat** command in Privileged EXEC mode to display the results of packet rate and loss information from the results buffer pool of the router after execution/completion of a **mstat** command. Within two minutes of completing the mstat command, the results are available in the buffer pool. The next **mstat** command overwrites the buffer pool with fresh results.

Syntax

show mstat

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the results of packet rate and loss information.

```
console#show mstat

Results for 'show mstat 0.0.0.0'
```

show mtrace

Use the **show mtrace** command in Privileged EXEC mode to display results of multicast trace path from the results buffer pool of the router after the execution/completion of a **mtrace** command. The results will be available in the buffer pool within two minutes of completing the command. A subsequent **mtrace** command overwrites the results in the buffer pool.

Syntax

show mtrace

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the results of packet rate and loss information.

```
console#show mtrace

Results for 'show mtrace 0.0.0.0'

Hops Away From Intermediate   Mcast Protocol TTL      Time Elapsed

Destination     Router Address In Use        Threshold Between Hops(msecs)

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

0              0.0.0.0
```

50

OSPF Commands

area default-cost

Use the **area default-cost** command in Router OSPF Configuration mode to configure the monetary default cost for the stub area. Use the no form of the command to return the cost to the default value.

Syntax

area *area-id* **default-cost** *integer*

no area *area-id* **default-cost**

- *area-id*—Identifies the OSPF stub area to configure. (Range: IP address or decimal from 0-4294967295)
- *integer*—The default cost for the stub area. (Range: 1-16777215)

Default Configuration

10 is the default configuration for *integer*.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example identifies a stub area of 10 and default cost of 100.

```
console(config)#router ospf
console(config-router)#area 10 default-cost 100
```

area nssa

Use the **area nssa** command in Router OSPF Configuration mode to configure the specified area ID to function as an NSSA. Use the no form of the command to disable NSSA from the specified area ID.

Syntax

area *area-id* **nssa**

no area *area-id* **nssa**

- *area-id*—Identifies the OSPF not-so-stubby-area. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures not-so-stubby-area 10 as an NSSA.

```
console(config)#router ospf
console(config-router)#area 10 nssa
```

area nssa default-info-originate

Use the **area nssa default-info-originate** command in Router OSPF Configuration mode to configure the metric value and type for the default route advertised into the NSSA. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2). Use the no form of the command to return the metric value and type to the default value.

Syntax

area *area-id* **nssa default-info-originate** [*integer*] [{**comparable | non-comparable**}]

no area *area-id* **nssa default-info-originate**

- *area-id*—Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0-4294967295)
- *integer*—Specifies the metric of the default route advertised to the NSSA. (Range: 1-16777214)
- **comparable**—A metric type of nssa-external 1

- **non-comparable**—A metric type of nssa-external 2

Default Configuration

If no metric is defined, 10 is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the metric value and type for the default route advertised into the NSSA.

```
console(config-router)#area 20 nssa default-info-originate 250
non-comparable
```

area nssa no-redistribute

Use the **area nssa no-redistribute** command in Router OSPF Configuration mode to configure the NSSA Area Border router (ABR) so that learned external routes are not redistributed to the NSSA.

Syntax

area *area-id* **nssa no-redistribute**

no area *area-id* **nssa no-redistribute**

- *area-id*—Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the NSSA ABR.

```
console(config-router)#area 20 nssa no-redistribute
```

area nssa no-summary

Use the **area nssa no-summary** command in Router OSPF Configuration mode to configure the NSSA so that summary LSAs are not advertised into the NSSA.

Syntax

area *area-id* **nssa no-summary**

no area *area-id* **nssa no-summary**

- *area-id*—Identifies the OSPF NSSA to configure. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the NSSA so that summary LSAs are not advertised into the NSSA.

```
console(config-router)#area 20 nssa no-summary
```

area nssa translator-role

Use the **area nssa translator-role** command in Router OSPF Configuration mode to configure the translator role of the NSSA.

Syntax

area *area-id* **nssa translator-role** {**always** | **candidate**}

no area *area-id* **nssa translator-role**

- *area-id*—Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0-4294967295)
- **always**—The router assumes the role of the translator when it becomes a border router.
- **candidate**—The router to participate in the translator election process when it attains border router status.

Default Configuration

The default role is candidate.

Command Mode
Router OSPF Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example configures the translator role of the NSSA.

```
console(config-router)#area 20 nssa translator-role always
```

area nssa translator-stab-intv

Use the **area nssa translator-stab-intv** command in Router OSPF Configuration mode to configure the translator stability interval of the NSSA.

Syntax

area *area-id* **nssa translator-stab-intv** *integer*

no area *area-id* **nssa translator-stab-intv**

- *area-id*—Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0-4294967295)
- *integer*—The period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router. (Range: 0-3600)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPF Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example configures the translator stability interval of the area 20 NSSA.

```
console(config-router)#area 20 nssa translator-stab-intv 2000
```

area range

Use the **area range** command in Router OSPF Configuration mode to configure a summary prefix for routes learned in a given area. There are two types of area ranges. An area range can be configured to summarize intra-area routes. An ABR advertises the range rather than the specific intra-area route as a type 3 summary LSA. Also, an area range can be configured at the edge of an NSSA to summarize external routes reachable within the NSSA. The range is advertised as a type 5 external LSA.

Syntax

area area-id **range** ip-address subnet-mask {**summarylink | nssaexternallink**} [**advertise |not-advertise**]

no area *area-id* **range** *ip-address subnet-mask* {**summarylink | nssaexternallink**}

- *area-id*—Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0-4294967295)
- *ip-address*—IP address.
- *subnet-mask*—Subnet mask associated with IP address.
- **summarylink**—Specifies a summary link LSDB type.
- **nssaexternallink**—Specifies an NSSA external link LSDB type.
- **advertise**—Advertisement of the area range.
- **notadvertise**—Suppresses advertisement of the area range.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

Use this command with Area Border Routers (ABRs).

Example

The following example defines an area range for the area 20.

```
console(config-router)#area 20 range 192.168.6.0 255.255.255.0
summarylink advertise
```

area stub

Use the **area stub** command in Router OSPF Configuration mode to create a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area. Use the no form of the command to remove the stub area.

Syntax

area *area-id* **stub**

no area *area-id* **stub**

- *area-id*—Identifies the area identifier of the OSPF stub. (Range: IP address or decimal from 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following examples define area 3 for the stub and then removes the stub area.

```
console(config-router)#area 3 stub
console(config-router)#no area 3 stub
```

area stub no-summary

Use the **area stub no-summary** command in Router OSPF Configuration mode to prevent Summary LSAs from being advertised into the NSSA. Use the no form of the command to return the Summary LSA mode to the default value.

Syntax

area *area-id* **stub no-summary**

no area *area-id* **stub no-summary**

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or decimal from 0-4294967295)

Default Configuration

Disabled is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example prevents the Summary LSA from being advertised into the area 3 NSSA.

```
console(config-router)#area 3 stub no-summary
```

area virtual-link

Use the **area virtual-link** command in Router OSPF Configuration mode to create the OSPF virtual interface for the specified area-id and neighbor router. To remove the link, use the no form of the command.

Syntax

area *area-id* **virtual-link** *neighbor-id*

no area *area-id* **virtual-link** *neighbor-id*

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or decimal from 0-4294967295)
- *neighbor-id*—Valid IP address.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example creates an OSPF virtual interface for area 10 and neighbor router.

```
console(config-router)#area 10 virtual-link 192.168.2.2
```

area virtual-link authentication

Use the **area virtual-link authentication** command in Router OSPF Configuration mode to configure the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the authentication type to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **authentication** {**none** | **simple** *key* |**encrypt** *key key-id*}

no area *area-id* **virtual-link** *neighbor-id* **authentication**

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or decimal from 0-4294967295)
- *neighbor-id*—Identifies the Router identifier of the neighbor.
- **encrypt**—Use MD5 Encryption for an OSPF Virtual Link.
- *key*—Authentication key for the specified interface. (Range: 8 bytes or less if the authentication type is **simple** and 16 bytes or less if the type is **encrypt**.)
- *key-id*—Authentication key identifier for the authentication type **encrypt**. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

Unauthenticated interfaces do not need an authentication key.

Example

The following example configures the authentication type and key for the area 10 OSPF virtual interface and neighbor ID.

```
console(config-router)#area 10 virtual-link 192.168.2.2
authentication encrypt test123 100
```

area virtual-link dead-interval

Use the **area virtual-link dead-interval** command in Router OSPF Configuration mode to configure the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router. Use the no form of the command to return the dead interval to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **dead-interval** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **dead-interval**

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or decimal from 0-4294967295)
- *neighbor-id*—Identifies the Router ID of the neighbor.
- *seconds*—Number of seconds to wait before the OSPF virtual interface on the virtual interface is assumed to be dead. (Range: 1-2147483647)

Default Configuration

40 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the dead interval for the area 10 OSPF virtual interface on the virtual interface and neighbor router.

```
console(config-router)#area 10 virtual-link 192.168.2.2 dead-
interval 655555
```

area virtual-link hello-interval

Use the **area virtual-link hello-interval** command in Router OSPF Configuration mode to configure the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the hello interval to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **hello-interval** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **hello-interval**

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or decimal from 0-4294967295)
- *neighbor-id*—Identifies the Router ID of the neighbor.
- *seconds*—Number of seconds to wait before sending hello packets to the OSPF virtual interface. (Range: 1-65535)

Default Configuration

10 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 50-second wait interval.

```
console(config-router)#area 10 virtual-link 192.168.2.2 hello-
interval 50
```

area virtual-link retransmit-interval

Use the **area virtual-link retransmit-interval** command in Router OSPF Configuration mode to configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the retransmit interval to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **retransmit-interval** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **retransmit-interval**

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or or decimal from 0-4294967295)
- *neighbor-id*—Identifies the Router ID of the neighbor.
- *seconds*—The number of seconds to wait between retransmitting LSAs if no acknowledgement is received. (Range: 1-3600)

Default Configuration

5 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 500-second retransmit wait interval.

```
console(config-router)#area 10 virtual-link 192.168.2.2
retransmit-interval 500
```

area virtual-link transmit-delay

Use the **area virtual-link transmit-delay** command in Router OSPF Configuration mode to configure the transmit delay for the OSPF virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the transmit delay to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **transmit-delay** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **transmit-delay**

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or or decimal from 0-4294967295)
- *neighbor-id*—Identifies the Router ID of the neighbor.
- *seconds*—Number of seconds to increment the age of the LSA before sending, based on the estimated time it takes to transmit from the interface. (Range: 0-3600)

Default Configuration

1 second is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 40-second transmit-delay interval.

```
console(config-router)#area 10 virtual-link 192.168.2.2 tranmit-
delay 40
```

default-information originate

Use the **default-information originate** command in Router OSPF Configuration mode to control the advertisement of default routes. Use the **no** form of the command to return the default route advertisement settings to the default value.

Syntax

default-information originate [**always**] [**metric** *integer*] [**metric-type** {**1** | **2**}]

no default-information originate [**metric**] [**metric-type**]

- **always**—Always advertise default routes.
- *integer*—The metric (or preference) value of the default route. (Range: 1-16777214)
- **1**—External type-1 route.
- **2**—External type-2 route.

Default Configuration

The default metric is none and the default type is 2.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example always advertises default routes.

```
console(config-router)#default-information originate always metric
100 metric-type 1
```

default-metric

Use the **default-metric** command in Router OSPF Configuration mode to set a default for the metric of distributed routes. Use the no form of the command to remove the metric from the distributed routes.

Syntax

default-metric *integer*

no default-metric

- *integer*—The metric (or preference) value of the default route. (Range: 1-16777214)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets a value of 50 for the default metric.

```
console(config-router)#default-metric 50
```

distance ospf

Use the **distance ospf** command in Router OSPF Configuration mode to set the route preference value of OSPF in the router. The range for the spectrum **intra/inter/type1/type2** is 2-255, but values must be assigned so that **intra<inter<type1<type2**. Use the no form of the command to return the specified metric to its default value.

Syntax

distance ospf {**intra** |**inter** \ **type1** | **type2**} *integer*

no distance ospf {**intra** |**inter** \ **type1** | **type2**}

- *integer*—The preference of the route. Lower route preference values are preferred when determining the best route. (Range: 2-255)

Default Configuration

intra: 8, inter: 10, type1: 13, type2: 150

Command Mode

Router OSPF Configuration mode

User Guidelines

The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.

Examples

The following examples set route preference values of OSPF in the router.

```
console(config-router)#distance ospf intra 4

console(config-router)#distance ospf type1 19
```

distribute-list out

Use the **distribute-list out** command in Router OSPF Configuration mode to specify the access list to filter routes received from the source protocol. Use the no form of the command to remove the specified source protocol from the access list.

Syntax

distribute-list *accesslistname* **out** {**rip**|**static** \ **connected**}

no distribute-list *accesslistname* **out {rip|static \ connected}**

- *accesslistname*—The name used to identify an existing ACL. The range is 1-31 characters.
- **rip**—Apply the specified access list when RIP is the source protocol.
- **static**—Apply the specified access list when packets come through the static route.
- **connected**—Apply the specified access list when packets come from a directly connected route.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the access list to filter routes received from the RIP source protocol.

```
console(config-router)#distribute-list ACL40 out rip
```

enable

Use the **enable** command in Router OSPF Configuration mode to reset the default administrative mode of OSPF in the router (active). Use the no form of the command to disable the administrative mode for OSPF.

Syntax

enable

no enable

Default Configuration

Enabled is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF router mode.

```
console(config-router)#enable
```

exit-overflow-interval

Use the **exit-overflow-interval** command in Router OSPF Configuration mode to configure the exit overflow interval for OSPF. When a router leaves the overflow state it can originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted. Use the no form of the command to return the interval to the default value.

Syntax

exit-overflow-interval *seconds*

no exit-overflow-interval

- *seconds*—Number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. (Range: 0-2147483647)

Default Configuration

0 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the exit overflow interval for OSPF at 10 seconds.

```
console(config-router)#exit-overflow-interval 10
```

external-lsdb-limit

Use the **external-lsdb-limit** command in Router OSPF Configuration mode to configure the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. Use the no form of the command to return the limit to the default value.

Syntax

external-lsdb-limit *integer*

no external-lsdb-limit

- *integer*—Maximum number of non-default ASexternal-LSAs allowed in the router's link-state database. (Range: -1 to 2147483647)

Default Configuration

-1 is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

Example

The following example configures the external LSDB limit for OSPF with the number of non-default ASexternal-LSAs set at 20.

```
console(config-router)#external-lsdb-limit 20
```

ip ospf

Use the **ip ospf** command in Interface Configuration mode to enable OSPF on a router interface. Use the no form of the command to disable OSPF on the interface.

Syntax

ip ospf

no ip ospf

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF on VLAN interface 15.

```
console(config-if-vlan15)#ip ospf
```

ip ospf areaid

Use the **ip ospf areaid** command in Interface Configuration mode to set the OSPF area to which the specified router interface belongs. Assigning an area ID, which does not exist on an interface, causes the area to be created with default values. The **no** version of this command removes the OSPF area setting for the specified router interface.

Syntax

ip ospf areaid *area-id*

no ip ospf areaid *area-id*

- *area-id*—Identifies the OSPF area to configure. (Range: IP address or or decimal from 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets area 10 as the the OSPF area to which the VLAN 15 router interface belongs.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip ospf areaid 10
```

ip ospf authentication

Use the **ip ospf authentication** command in the Interface Configuration mode to set the OSPF Authentication Type and Key for the specified interface. Use the no form of the command to return the authentication type to the default value.

Syntax

ip ospf authentication {**none** | {**simple** *key*} | {**encrypt** *key key-id*}}

no ip ospf authentication

- **encrypt**—MD5 encrypted authentication key.
- *key*—Authentication key for the specified interface. (Range: 8 bytes or less if the authentication type is **simple** and 16 bytes or less if the type is **encrypt**.)

- *key-id*—Authentication key identifier for the authentication type **encrypt**. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Unauthenticated interfaces do not need an authentication key or authentication key ID.

Example

The following example sets the OSPF Authentication Type and Key for VLAN 15.

```
console(config-if-vlan15)#ip ospf authentication encrypt test123
100
```

ip ospf cost

Use the **ip ospf cost** command in Interface Configuration mode to configure the cost on an OSPF interface. Use the no form of the command to return the cost to the default value.

Syntax

ip ospf cost *integer*

no ip ospf cost

- *integer*—Specifies the cost (link-state metric) of the OSPF interface. (Range: 1-65535)e

Default Configuration

10 is the default link-state metric configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the cost on the OSPF interface at 5.

```
console(config-if-vlan15)#ip ospf cost 5
```

ip ospf dead-interval

Use the **ip ospf dead-interval** command in Interface Configuration to set the OSPF dead interval for the specified interface. Use the no form of the command to return the interval to the default value.

Syntax

ip ospf dead-interval *seconds*

no ip ospf dead-interval

- *seconds*—Number of seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. (Range: 1-65535)

Default Configuration

40 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4).

Example

The following example sets the dead interval at 30 seconds.

```
console(config-if-vlan15)#ip ospf dead-interval 30
```

ip ospf hello-interval

Use the **ip ospf hello-interval** command in Interface Configuration mode to set the OSPF hello interval for the specified interface. Use the no form of the command to return the interval to the default value.

Syntax

ip ospf hello-interval *seconds*

no ip ospf hello-interval

- *seconds*—Number of seconds to wait before sending Hello packets from the interface. (Range: 1-65535)

Default Configuration

10 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The value for the length of time must be the same for all routers attached to a network.

Example

The following example sets the OSPF hello interval at 30 seconds.

```
console(config-if-vlan15)#ip ospf hello-interval 30
```

ip ospf mtu-ignore

Use the **ip ospf mtu-ignore** command in Interface Configuration mode to disable OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established. Use the no form of the command to enable OSPF maximum transmission unit (MTU) mismatch detection.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example disables OSPF MTU mismatch detection on VLAN interface 15.

```
console(config-if-vlan15)#ip ospf mtu-ignore
```

ip ospf priority

Use the **ip ospf priority** command in Interface Configuration mode to set the OSPF priority for the specified router interface. Use the no form of the command to return the priority to the default value.

Syntax

ip ospf priority *integer*

no ip ospf priority

- *integer*—Specifies the OSPF priority for the specified router interface. (Range: 0-255)

Default Configuration

1 is the default integer value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

A value of 1 is the highest router priority. A value of 0 indicates that the interface is not eligible to become the designated router on this network.

Example

The following example sets the OSPF priority for the VLAN 15 router at 100.

```
console(config-if-vlan15)#ip ospf priority 100
```

ip ospf retransmit-interval

Use the **ip ospf retransmit-interval** command in Interface Configuration mode to set the OSPF retransmit Interval for the specified interface. Use the no form of the command to return the interval to the default value.

Syntax

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

- *seconds*—Number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. (Range: 0-3600 seconds)

Default Configuration

5 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

A value of 1 is the highest router priority. A value of 0 indicates that the interface is not eligible to become the designated router on this network.

Example

The following example sets the OSPF retransmit Interval for VLAN 15 at 50 seconds.

```
console(config-if-vlan15)#ip ospf retransmit-interval 50
```

ip ospf transmit-delay

Use the **ip ospf transmit-delay** command in Interface Configuration mode to set the OSPF Transit Delay for the specified interface. Use the no form of the command to return the delay to the default value.

Syntax

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

- *seconds*—Sets the estimated number of seconds it takes to transmit a link state update packet over this interface. (Range: 1-3600 seconds)

Default Configuration

1 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF Transit Delay for VLAN 15 at 20 seconds.

```
console(config-if-vlan15)#ip ospf transmit-delay 20
```

maximum-paths

Use the **maximum-paths** command in Router OSPF Configuration mode to set the number of paths that OSPF can report for a given destination. Use the no form of the command to reset the number to the default value.

Syntax

maximum-paths *integer*

no maximum-paths

- *integer*—Number of paths that OSPF can report for a given destination. (Range is 1-2.)

Default Configuration

2 is the *integer* default value.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of paths at 2 that OSPF can report for a given destination.

```
console(config-router)#maximum-paths 2
```

redistribute

Use the **redistribute** command in Router OSPF Configuration mode to configure OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Syntax

Use the no version of the command to disable redistribution from the selected source or to reset options to their default values.

redistribute {**rip | static | connected**} [**metric** *integer*] [**metric-type** {**1 | 2**}] [**tag** *integer*] [**subnets**]

no redistribute {**rip | static | connected**} [**metric** *integer*] [**metric-type** {**1 | 2**}] [**tag** *integer*] [**subnets**]

- **rip—** Specifies RIP as the source protocol.
- **static—**Specifies that the source is a static route.
- **connected—**Specifies that the source is a directly connected route.
- **metric—**Specifies the metric to use when redistributing the route. (Range: 0-16777214)
- **metric-type 1—**Type 1 external route.
- **metric-type 2—**Type 2 external route.
- **tag—**Value attached to each external route, which might be used to communicate information between ASBRs. (Range: 0-4294967295)
- **subnets—**Specifies whether to redistribute the routes to subnets.

Default Configuration

0 is the tag integer default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

```
console(config-router)#redistribute rip metric 90 metric-type 1
tag 555 subnets
```

router-id

Use the **router-id** command in Router OSPF Configuration mode to set a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.

Syntax

router-id *ip-address*

- *ip-address*—IP address that uniquely identifies the router OSPF ID.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines the router OSPF ID as 5.5.5.5 .

```
console(config)#router ospf
console(config-router)#router-id 5.5.5.5
```

router ospf

Use the **router ospf** command in Global Configuration mode to enter Router OSPF mode.

Syntax

router ospf

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The command prompt changes when the **router ospf** command executes.

Example

The following example enters into router OSPF mode.

```
console(config)#router ospf
console(config-router)#
```

show ip ospf

Use the **show ip ospf** command in Privileged EXEC mode to display information relevant to the OSPF router.

Syntax

show ip ospf

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays OSPF router information.

```
console#show ip ospf
Router ID..................................... 5.5.5.5
OSPF Admin Mode............................... Enable
ASBR Mode..................................... Enable
RFC 1583 Compatibility........................ Enable
ABR Status.................................... Disable
Exit Overflow Interval........................ 0
Spf Delay Time................................ 20
Spf Hold Time................................. 30
External LSA Count............................ 0
```

```
External LSA Checksum..................... 0
New LSAs Originated....................... 0
LSAs Received............................. 0
External LSDB Limit....................... No Limit
Default Metric............................ Not configured
Default Route Advertise................... Enabled
Always.................................... TRUE
Metric.................................... 100
Metric Type............................... External Type 1
Maximum Paths............................. 2
Redistributing.............................
Source.................................... rip
Metric.................................... 90
Metric Type............................... 1
Tag....................................... 555
Subnets................................... Yes
Distribute List........................... ACL2
```

show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

Syntax

show ip ospf abr

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode
User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip ospf abr

Type Router Id   Cost  Area ID         Next Hop    Next Hop
                                                   Intf
----- ---------  ----- --------------- ---------   --------
INTRA 3.3.3.3    1     0.0.0.1         10.1.23.3   vlan11
INTRA 4.4.4.4    10    0.0.0.1         10.1.24.4   vlan12
```

show ip ospf area

Use the **show ip ospf area** command in Privileged EXEC mode to display information about the identified OSPF area.

Syntax

show ip ospf area *area-id*

- *area-id*—Identifies the OSPF area whose ranges are being displayed. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays OSPF router information.

```
console#show ip ospf area 10

AreaID..................................... 0.0.0.10

External Routing........................... Import External
LSAs

Spf Runs................................... 0

Area Border Router Count................... 0

Area LSA Count............................. 0
```

```
Area LSA Checksum.............................. 0
Import Summary LSAs............................ Enable
console#show ip ospf area 20
AreaID......................................... 0.0.0.20
External Routing............................... Import NSSAs
Spf Runs....................................... 0
Area Border Router Count....................... 0
Area LSA Count................................. 0
Area LSA Checksum.............................. 0
OSPF NSSA Specific Information.
Import Summary LSAs............................ Enable
Redistribute into NSSA......................... Enable
Default Information Originate.................. TRUE
Default Metric................................. 250
Default Metric Type............................ Non-Comparable
Translator Role................................ Candidate
Translator Stability Interval.................. 2000
Translator State............................... Disabled
```

show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR). This command takes no options.

Syntax

show ip ospf asbr

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode
User EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#show ip ospf asbr

Type  Router Id   Cost  Area ID    Next Hop    Next Hop
                                                Intf

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

INTRA  1.1.1.1     1     0.0.0.1   10.1.12.1    vlan10

INTRA  4.4.4.4     10    0.0.0.1   10.1.24.4    vlan12
```

show ip ospf database

Use the **show ip ospf database** command in Privileged EXEC mode to display information about the link state database when OSPF is enabled. If parameters are entered, the command displays the LSA headers. Use the optional parameters to specify the type of link state advertisements to display.

Syntax

show ip ospf [*<area-id>*] **database** [{**asbr-summary** | **external** | **network** | **nssa-external** | **router** | **summary**}][*ls-id*] [**adv-router** [*ip-address*] | **self-originate**]

- *area-id*—Identifies a specific OSPF area for which link state database information will be displayed.
- **asbr-summary**—Display the autonomous system boundary router (ASBR) summary LSAs.
- **external**—Display the external LSAs.
- **network**—Display the network LSAs.
- **nssa-external**—Display NSSA external LSAs.
- **router**—Display router LSAs.
- **summary**—Display the LSA database summary information.
- *ls-id*—Specifies the link state ID (LSID). (Range: IP address or an integer in the range of 0-4294967295)
- **adv-router**—Display the LSAs that are restricted by the advertising router. To specify a router, enter the IP address of the router.
- **self-originate**—Display the LSAs in that are self-originated.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Information is only displayed if OSPF is enabled.

Example

The following example displays information about the link state database when OSPF is enabled.

```
console#show ip ospf database router 10 adv-router 192.168.7.7

The Link State Database is empty.
```

show ip ospf database database-summary

Use the **show ip ospf database database-summary** command in Privileged EXEC mode to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

Syntax

show ip ospf database database-summary

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the number of each type of LSA in the database for each area and for the router.

```
console#show ip ospf database database-summary

OSPF Router with ID (5.5.5.5)

Area 0.0.0.0 database summary

Router.......................................... 0
```

```
Network..................................... 0
Summary Net................................. 0
Summary ASBR................................ 0
Type-7 Ext.................................. 0
Self Originated Type-7...................... 0
Opaque Link................................. 0
Opaque Area................................. 0
Subtotal.................................... 0
Area 0.0.0.10 database summary
Router...................................... 0
Network..................................... 0
Summary Net................................. 0
Summary ASBR................................ 0
Type-7 Ext.................................. 0
Self Originated Type-7...................... 0
Opaque Link................................. 0
Opaque Area................................. 0
Subtotal.................................... 0
Router database summary
Router...................................... 0
Network..................................... 0
Summary Net................................. 0
Summary ASBR................................ 0
Type-7 Ext.................................. 0
Opaque Link................................. 0
Opaque Area................................. 0
Type-5 Ext.................................. 0
Self-Originated Type-5 Ext.................. 0
Opaque AS................................... 0
```

```
Total..................................... 0
```

show ip ospf interface

Use the **show ip ospf interface** command in Privileged EXEC mode to display the information for the VLAN or loopback interface.

Syntax

show ip ospf interface {**vlan** *vlan-id* | **loopback** *loopback-id*}

- *vlan-id*—Valid VLAN ID.
- *loopback-id*—Shows information the specified loopback interface. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the information for the IFO object or virtual interface tables associated with VLAN 3.

```
console#show ip ospf interface vlan 3


IP Address..................................... 3.1.1.2
Subnet Mask.................................... 255.255.255.0
Secondary IP Address(es).......................
OSPF Admin Mode................................ Enable
OSPF Area ID................................... 0.0.0.1
Router Priority................................ 1
Retransmit Interval............................ 5
Hello Interval................................. 10
Dead Interval.................................. 40
LSA Ack Interval............................... 1
```

```
Iftransit Delay Interval..................... 1
Authentication Type.......................... None
Metric Cost.................................. 10  (computed)
OSPF Mtu-ignore.............................. Disable
OSPF Interface Type.......................... broadcast
State................................... backup-designated-router
Designated Router............................ 3.1.1.1
Backup Designated Router..................... 3.1.1.2
Number of Link Events........................ 2
```

show ip ospf interface brief

Use the **show ip ospf interface brief** command in Privileged EXEC mode to display brief information for the IFO object or virtual interface tables.

Syntax

show ip ospf interface brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays brief information for the IFO object or virtual interface tables.

```
console#show ip ospf interface brief
Router Hello Dead Retrax Retrax LSAAck
Interface AdminMode Area ID Priority Intval Intval Intval Delay Intval
--------- --------- ------- -------- ------ ------ ------ ----- ------
vlan1     Enable    0.0.0.10 1       10     40     5      1     1
vlan2     Disable   0.0.0.0  1       10     40     5      1     1
vlan3     Disable   0.0.0.0  1       10     40     5      1     1
```

```
loopback2 Disable   0.0.0.0  1       10     40     5      1     1
```

show ip ospf interface stats

Use the show ip ospf interface stats command in User EXEC mode to display the statistics for a specific interface. The information is only displayed if OSPF is enabled.

Syntax

show ip ospf interface stats vlan *vlan-id*

- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the ospf statistics for VLAN 15.

```
console>show ip ospf interface stats vlan15

OSPF Area ID..................................... 0.0.0.0

Area Border Router Count..................... 0

AS Border Router Count....................... 0

Area LSA Count.................................. 1

IP Address.....................................2.2.2.2

OSPF Interface Events........................... 1

Virtual Events.................................. 0

Neighbor Events................................. 0

External LSA Count.............................. 0
```

show ip ospf neighbor

Use the **show ip ospf neighbor** command in Privileged EXEC mode to display information about OSPF neighbors. The information below only displays if OSPF is enabled and the interface has a neighbor.

Syntax

show ip ospf neighbor [**interface vlan** *vlan-id*] [*ip-address*]

- *vlan-id*—Valid VLAN ID.
- *ip-address*—Valid IP address of the neighbor.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display information about OSPF neighbors on the specified Ethernet and IP interfaces.

```
console#show ipv6 ospf neighbor interface tunnel 1


Router ID   Priority   Intf  Interface   State          Dead

                        ID                               Time

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

4.1.0.0     0          13    tunnel 1    Full/DR-OTHER  30
```

show ip ospf range

Use the **show ip ospf range** command in Privileged EXEC mode to display information about the area ranges for the specified area-id.

Syntax

show ip ospf range *area-id*

- *area-id*—Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the area ranges for the specified area-id.

```
console#show ip ospf range 20

Area ID  IP Address  Subnet Mask   Lsdb Type    Advertisement

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

0.0.0.20 192.168.6.0 255.255.255.0 Summary Link Enabled
```

show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

Syntax

show ip ospf statistics

Default Configuration

This command has no default configuration.

Command Mode

User EXEC

User Guidelines

This command has no user guidelines.

Example

```
console>show ip ospf statistics

Area 0.0.0.0: SPF algorithm executed 0 times

Delta T   SPF Duration (msec)        Reason

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

26:01:45                   0

23:15:05                   0    R

23:14:22                   0    R, N

23:14:12                   0    R

23:10:04                   0
```

show ip ospf stub table

Use the **show ip ospf stub table** command in Privileged EXEC mode to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Syntax

show ip ospf stub table

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
console(config)#show ip ospf stub table

AreaId           TypeofService Metric Val  Import SummaryLSA


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


0.0.0.1          Normal           1              Enable
```

show ip ospf virtual-link

Use the **show ip ospf virtual-link** command in Privileged EXEC mode to display the OSPF Virtual Interface information for a specific area and neighbor.

Syntax

show ip ospf virtual-link *area-id neighbor-id*

- *area-id*—Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0-4294967295)
- *neighbor-id*—Identifies the neighbor's router ID. (Range: Valid IP address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information for area 10 and its neighbor.

```
console#show ip ospf virtual-link 10 192.168.2.2

Area ID..................................... 10

Neighbor Router ID.......................... 192.168.2.2

Hello Interval.............................. 10

Dead Interval............................... 655555

Iftransit Delay Interval.................... 1

Retransmit Interval......................... 5

State....................................... down

Metric...................................... 0

Neighbor State.............................. down

Authentication Type......................... MD5

Authentication Key.......................... "test123"

Authentication Key ID....................... 100
```

show ip ospf virtual-link brief

Use the **show ip ospf virtual-link brief** command in Privileged EXEC mode to display the OSPF Virtual Interface information for all areas in the system.

Syntax

show ip ospf virtual-link brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information for all areas in the system.

```
console#show ipv6 ospf virtual-link brief
                      Hello    Dead     Retransmit  Transit
Area ID  Neighbor     Interval Interval Interval    Delay
-------  --------     -------- -------- ----------  --------
0.0.0.2  5.5.5.5      10       40       5           1
```

timers spf

Use the **timers spf** command in Router OSPF Configuration mode to configure the SPF delay and hold time. Use the no form of the command to reset the numbers to the default value.

Syntax

timers spf *delay-time hold-time*

no timers spf

- *delay-time*—SPF delay time. (Range: 0-65535 seconds)
- *hold-time*—SPF hold time. (Range: 0-65535 seconds)

Default Configuration

5 is the *delay-time* default value. 10 is the *hold-time* default value.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the SPF delay and hold time.

```
console(config-router)#timers spf 20 30
```

trapflags

Use the **trapflags** command in Router OSPF Configuration mode to enable OSPF traps. Use the no form of the command to disable OSPF traps.

Syntax

trapflags

no trapflags

Default Configuration

Enabled is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF traps.

```
console(config-router)#trapflags
```

1583compatibility

Use the **1583compatibility** command in Router OSPF Configuration mode to enable OSPF 1583 compatibility. Use the no form of the command to disable it.

Syntax

1583compatibility

no 1583compatibility

Default Configuration

Enabled is the default configuration.

Command Mode

Router OSPF Configuration mode

User Guidelines

If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Example

```
The following example enables 1583 compatibility.

console(config-router)#1583compatibility
```

51

OSPFv3 Commands

area default-cost

Use the **area default-cost** command in Router OSPFv3 Configuration mode to configure the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777215. Use the no form of the command to return the cost to the default value.

Syntax

area *areaid* **default-cost** *cost*

no area *areaid* **default-cost**

- *areaid*—Valid area identifier.
- *cost*—Default cost. (Range: 1-16777215)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the monetary default cost at 100 for stub area 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 default-cost 100
```

area nssa

Use the **area nssa command** in Router OSPFv3 Configuration mode to configure the specified areaid to function as an NSSA.

Syntax

area *areaid* **nssa**

no area *areaid* **nssa**

- *areaid*—Valid OSPFv3 area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures area 1 to function as an NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa
```

area nssa default-info-originate

Use the **area nssa default-info-originate** command in Router OSPFv3 Configuration mode to configure the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route. The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2). Use the **no** form of the command to return the metric value and type to the default value

Syntax

area *areaid* **nssa default-info-originate** [*metric* [**comparable | non-comparable**]]

no area *areaid* **nssa default-info-originate**

- *areaid*—Valid OSPFv3 area identifier.
- *metric*—Metric value for default route. (Range: 1-16777215)
- **comparable**—Metric Type (nssa-external 1). (Range: 1-16777214)
- **non-comparable**—Metric Type (nssa-external 2). (Range: 1-16777214)

Default Configuration

If no metric is defined, 10 is the default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the default metric value for the default route advertised into the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa default-info-originate
```

area nssa no-redistribute

Use the **area nssa no-redistribute** command in Router OSPFv3 Configuration mode to configure the NSSA ABR so that learned external routes will not be redistributed to the NSSA. Use the **no** form of the command to remove the configuration.

Syntax

area *areaid* **nssa no-redistribute**

no area *areaid* **nssa no-redistribute**

- *areaid*—Valid OSPF area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the area 1 NSSA ABR so that learned external routes will not be redistributed to the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa no-redistribute
```

area nssa no-summary

Use the **area nssa no-summary** command in Router OSPFv3 Configuration mode to configure the NSSA so that summary LSAs are not advertised into the NSSA. Use the no form of the command to remove the configuration.

Syntax

area *areaid* **nssa no-summary**

no area *area-id* **nssa no-summary**

- *areaid*—Valid OSPF area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the area 1 NSSA so that summary LSAs are not advertised into the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa no-summary
```

area nssa translator-role

Use the **area nssa translator-role** command in Router OSPFv3 Configuration mode to configure the translator role of the NSSA. Use the **no** form of the command to remove the configuration.

Syntax

area *areaid* **nssa translator-role** {**always** | **candidate**}

no area *areaid* **nssa translator-role**

- *areaid*—Valid OSPF area identifier.
- **always**—Causes the router to assume the role of the translator the instant it becomes a border router.
- **candidate**—Causes the router to participate in the translator election process when it attains border router status.

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example configures the **always** translator role of the area 1 NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa translator-role always
```

area nssa translator-stab-intv

Use the **area nssa translator-stab-intv** command in Router OSPFv3 Configuration mode to configure the translator stability interval of the NSSA. The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Syntax
area *areaid* **nssa translator-stab-intv** *seconds*

no area *areaid* **nssa translator-stab-intv**

- *areaid*—Valid OSPF area identifier.
- *seconds*—Translator stability interval of the NSSA. (Range: 0-3600 seconds)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example configures a translator stability interval of 100 seconds for the area 1 NSSA.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#area 1 nssa translator-stab-intv 100
```

area range

Use the **area range** command in Router OSPF Configuration mode to configure a summary prefix for routes learned in a given area. There are two types of area ranges. An area range can be configured to summarize intra-area routes. An ABR advertises the range rather than the specific intra-area route as a type 3 summary LSA. Also, an area range can be configured at the edge of an NSSA to summarize external routes reachable within the NSSA. The range is advertised as a type 5 external LSA. Use the **no** form of the command to remove the summary prefix configuration for routes learned in the specified area.

Syntax

area *areaid* **range** *ipv6-prefix/prefix-length* {**summarylink | nssaexternallink**} [**advertise | not-advertise**]

no area *areaid* **range** *ipv6-prefix/prefix-length* {**summarylink | nssaexternallink**}

- *areaid*—Valid OSPF area identifier.
- *ipv6-prefix/prefix-length*—Valid route prefix.
- **summarylink**—LSDB type
- **nssaexternallink**—LSDB type.
- **advertise**—Allows area range to be advertised.
- **not-advertise**—Suppresses area range from being advertised.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

The LSDB type must be specified by either **summarylink** or **nssaexternallink**, and the advertising of the area range can be allowed or suppressed.

Example

The following example creates an area range for the area 1 NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 range 2020:1::1/64 summarylink
```

area stub

Use the **area stub** command in Router OSPFv3 Configuration mode to create a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Syntax

area *areaid* **stub**

no area *areaid* **stub**

- *areaid*—Valid OSPFv3 area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example creates a stub area for area 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 stub
```

area stub no-summary

Use the **area stub no-summary** command in Router OSPFv3 Configuration mode to disable the import of Summary LSAs for the stub area identified by *areaid*.

Syntax

area *areaid* **stub no-summary**

no area *areaid* **stub no-summary**

- *areaid*—Valid OSPFv3 area identifier.

Default Configuration

This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example prevents Summary LSAs from being advertised into the area 1 NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 stub no-summary
```

area virtual-link

Use the **area virtual-link** command in Router OSPFv3 Configuration mode to create the OSPF virtual interface for the specified *areaid* and *neighbor*. Use the **no area virtual-link** command to delete an OSPF virtual interface in an area.

Syntax
area *areaid* **virtual-link** *neighbor-id*

no area *areaid* **virtual-link** *neighbor-id*

- *areaid*—Valid OSPFv3 area identifier (or decimal value in the range of 0-4294967295).
- *neighbor-id*—Identifies the Router ID or IP address of the neighbor.

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example creates the OSPF virtual interface for area 1 and its neighbor router.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2
```

area virtual-link dead-interval

Use the **area virtual-link dead-interval** command in Router OSPFv3 Configuration mode to configure the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **dead-interval** *seconds*

no area *areaid* **virtual-link** *neighbor* **dead-interval**

- *areaid*—Valid OSPFv3 area identifier.
- *neighbor*—Router ID of neighbor.
- *seconds*—Dead interval. (Range: 1-65535)

Default Configuration

40 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 20-second dead interval for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 dead-interval 20
```

area virtual-link hello-interval

Use the **area virtual-link hello-interval** command in Router OSPFv3 Configuration mode to configure the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **hello-interval** *seconds*

no area *areaid* **virtual-link** *neighbor* **hello-interval**

- *areaid*—Valid OSPFv3 area identifier.
- *neighbor*—Router ID of neighbor.

- *seconds*—Hello interval. (Range: 1-65535)

Default Configuration

10 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a hello interval of 20 seconds for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 hello-interval 20
```

area virtual-link retransmit-interval

Use the **area virtual-link retransmit-interval** command in Router OSPFv3 Configuration mode to configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **retransmit-interval** *seconds*

no area *areaid* **virtual-link** *neighbor* **retransmit-interval**

- *areaid*—Valid OSPFv3 area identifier.
- *neighbor*—Router ID of neighbor.
- *seconds*—Retransmit interval. (Range: 0-3600)

Default Configuration

5 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the retransmit interval of 20 seconds for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
(config)#ipv6 router ospf
(config-rtr)#area 1 virtual-link 2 retransmit-interval 20
```

area virtual-link transmit-delay

Use the **area virtual-link transmit-delay** command in Router OSPFv3 Configuration mode to configure the transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **transmit-delay** *seconds*

no area *areaid* **virtual-link** *neighbor* **transmit-delay**

- *areaid*—Valid OSPFv3 area identifier.
- *neighbor*—Router ID of neighbor.
- *seconds*—Transmit delay interval. (Range: 0-3600)

Default Configuration

1 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 20-second transmit delay for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 transmit-delay 20
```

default-information originate

Use the **default-information originate** command in Router OSPFv3 Configuration mode to control the advertisement of default routes. Use the **no** form of the command to return the default route advertisement settings to the default value.

Syntax

default-information originate [**always**] [**metric** *integer*] [**metric-type** {**1** | **2**}]

no default-information originate [**metric**] [**metric-type**]

- **always** — Always advertise default routes.
- *integer* — The metric (or preference) value of the default route. (Range: 0-16777214)
- **1**—External type-1 route.
- **2**—External type-2 route.
- **metric** — Specify the metric of the default route.
- **metric-type** — Specify metric-type of the default route.

Default Configuration

2 is the default value for **metric-type**.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example controls the advertisement of default routes by defining a metric value of 100 and metric type 2.

```
console(config)#ipv6 router ospf

console(config-rtr)#default-information originate metric 100
metric-type 2
```

default-metric

Use the **default-metric** command in Router OSPFv3 Configuration mode to set a default for the metric of distributed routes.

Syntax

default-metric *metric*

no default-metric

- *metric*—Metric value used for distribution (Range: 1-16777214)

Default Configuration

This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example sets a default of 100 for the metric of distributed routes.

```
console(config)#ipv6 router ospf
console(config-rtr)#default-metric 100
```

distance ospf

Use the **distance ospf** command in Router OSPFv3 Configuration mode to set the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.

Syntax
distance ospf {**intra** | **inter** | **type1** | **type2**} *preference*

no distance ospf {**intra** | **inter** | **type1** | **type2**}

- *preference*—Route preference. (Range: 1-255)

Default Configuration
This command has no default configuration.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example sets a route preference value of 100 for intra OSPF in the router.

```
console(config)#ipv6 router ospf
console(config-rtr)#distance ospf intra 100
```

enable

Use the **enable** command in Router OSPFv3 Configuration mode to enable administrative mode of OSPF in the router (active).

Syntax

enable

no enable

Default Configuration

Enabled is the default state.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables administrative mode of OSPF in the router (active).

```
console(config)#ipv6 router ospf
console(config-rtr)#enable
```

exit-overflow-interval

Use the **exit-overflow-interval** command in Router OSPFv3 Configuration mode to configure the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to originate non-default AS-external-LSAs again. When set to 0, the router will not leave Overflow State until restarted.

Syntax

exit-overflow-interval *seconds*

no exit-overflow-interval

- *seconds*—Exit overflow interval for OSPF (Range: 0-2147483647)

Default Configuration

0 is the default value for *seconds*.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example configures the exit overflow interval for OSPF at 100 seconds.

```
console(config)#ipv6 router ospf
console(config-rtr)#exit-overflow-interval 100
```

external-lsdb-limit

Use the **external-lsdb-limit** command in Router OSPFv3 Configuration mode to configure the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default ASexternal- LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

Syntax
external-lsdb-limit *limit*

no external-lsdb-limit

- *limit*—External LSDB limit for OSPF (Range: -1-2147483647)

Default Configuration
-1 is the default value for *limit*.

Command Mode
Router OSPFv3 Configuration mode

User Guidelines
This command has no user guidelines.

Example
The following example sets the external LSDB limit at 100 for OSPF.

```
console(config)#ipv6 router ospf
console(config-rtr)#external-lsdb-limit 100
```

ipv6 ospf

Use the **ipv6 ospf** command in Interface Configuration mode to enable OSPF on a router interface or loopback interface.

Syntax

ipv6 ospf

no ipv6 ospf

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF on VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf
```

ipv6 ospf areaid

Use the **ipv6 ospf areaid** command in Interface Configuration mode to set the OSPF area to which the specified router interface belongs.

Syntax

ipv6 ospf areaid *areaid*

no ipv6 ospf areaid *areaid*

- *areaid*—Is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value. It uniquely identifies the area to which the interface connects. Assigning an area id which does not exist on an interface causes the area to be created with default values. (Range: 0-4294967295).

Default Configuration

This command has no default configuration.

Command Mode
Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines
This command has no user guidelines.

Example
The following example defines the OSPF area to which VLAN 15 belongs.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf areaid 100
```

ipv6 ospf cost

Use the **ipv6 ospf cost** command in Interface Configuration mode to configure the cost on an OSPF interface.

Syntax
ipv6 ospf cost *cost*

no ipv6 ospf cost

- *cost*—Cost for OSPF interface. (Range: 1-65535)

Default Configuration
10 is the default value of *cost*.

Command Mode
Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines
This command has no user guidelines.

Example
The following example configures a cost of 100.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf cost 100
```

ipv6 ospf dead-interval

Use the **ipv6 ospf dead-interval** command in Interface Configuration mode to set the OSPF dead interval for the specified interface.

Syntax

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval

- *seconds*—A valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). (Range: 1-65535)

Default Configuration

40 seconds is the default value of *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF dead interval at 100 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf dead-interval 100
```

ipv6 ospf hello-interval

Use the **ipv6 ospf hello-interval** command in Interface Configuration mode to set the OSPF hello interval for the specified interface.

Syntax

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

seconds—A valid positive integer which represents the length of time of the OSPF hello interval. The value must be the same for all routers attached to a network. (Range: 1-65535 seconds)

Default Configuration

10 seconds is the default value of *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF hello interval at 15 seconds.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 ospf hello-interval 15
```

ipv6 ospf mtu-ignore

Use the **ipv6 ospf mtu-ignore** command in Interface Configuration mode to disable OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Default Configuration

Enabled is the default state.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example disables OSPF maximum transmission unit (MTU) mismatch detection.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 ospf mtu-ignore
```

ipv6 ospf network

Use the **ipv6 ospf network** command in Interface Configuration mode to change the default OSPF network type for the interface. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF-type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Syntax

ipv6 ospf network { **broadcast** | **point-to-point** }

no ipv6 ospf network

- **broadcast**—The network type is broadcast.
- **point-to-point**—The network type is point-to-point.

Default Configuration

Broadcast is the default state.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example changes the default OSPF network type to point-to-point.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf network point-to-point
```

ipv6 ospf priority

Use the **ipv6 ospf priority** command in Interface Configuration mode to set the OSPF priority for the specified router interface.

Syntax

ipv6 ospf priority *priority*

no ipv6 ospf priority

- *priority*—OSPF priority for specified interface. (Range: 0-255. A value of 0 indicates that the router is not eligible to become the designated router on this network)

Default Configuration

1, the highest router priority, is the default value.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF priority at 50 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf priority 50
```

ipv6 ospf retransmit-interval

Use the **ipv6 ospf retransmit-interval** command in Interface Configuration mode to set the OSPF retransmit interval for the specified interface.

Syntax

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval

- *seconds*—The number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. (Range: 0 to 3600 seconds)

Default Configuration

5 seconds is the default value.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF retransmit interval at 100 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf retransmit-interval 100
```

ipv6 ospf transmit-delay

Use the **ipv6 ospf transmit-delay** command in Interface Configuration mode to set the OSPF Transmit Delay for the specified interface.

Syntax

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

- *seconds*—OSPF transmit delay for the specified interface. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. (Range: 1 to 3600 seconds)

Default Configuration

No default value.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF Transmit Delay at 100 seconds for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf transmit-delay 100
```

ipv6 router ospf

Use the **ipv6 router ospf** command in Global Configuration mode to enter Router OSPFv3 Configuration mode.

Syntax

ipv6 router ospf

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

Use the following command to enable OSPFv3.

```
console(config)#ipv6 router ospf
```

maximum-paths

Use the **maximum-paths** command in Router OSPFv3 Configuration mode to set the number of paths that OSPF can report for a given destination.

Syntax

maximum-paths *maxpaths*

no maximum-paths

- *maxpaths*—Number of paths that can be reported. (Range: 1-2)

Default Configuration

2 is the default value for *maxpaths*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of paths that OSPF can report for a given destination to 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#maximum-paths 1
```

redistribute

Use the **redistribute** command in Router OSPFv3 Configuration mode to configure the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

Syntax

redistribute {static | connected} [**metric** *metric*] [**metric-type** {**1** | **2**}] [**tag** *tag*]

no redistribute {static | connected} [**metric**] [**metric-type**] [**tag**]

- *metric*—Metric value used for default routes. (Range: 0-16777214)
- *tag*—Tag. (Range: 0-4294967295)

Default Configuration

2 is the default value for **metric-type,** 0 for *tag*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

```
console(config)#ipv6 router ospf
console(config-rtr)#redistribute connected
```

router-id

Use the **router-id** command in Router OSPFv3 Configuration mode to set a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.

Syntax

router-id *router-id*

- *router-id*—Router OSPF identifier. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets a 4-digit dotted-decimal number identifying the Router OSPF ID as 2.3.4.5.

```
console(config)#ipv6 router ospf
console(config-rtr)#router-id 2.3.4.5
```

show ipv6 ospf

Use the **show ipv6 ospf** command in Privileged EXEC mode to display information relevant to the OSPF router.

Syntax

show ipv6 ospf

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF traps.

```
console#show ipv6 ospf
Router ID..................................... 0.0.0.2
OSPF Admin Mode............................... Enable
ASBR Mode..................................... Disable
ABR Status.................................... Disable
Exit Overflow Interval........................ 0
External LSA Count............................ 0
External LSA Checksum......................... 0
New LSAs Originated........................... 0
LSAs Received................................. 0
External LSDB Limit........................... No Limit
```

```
Default Metric.............................. Not Configured
Maximum Paths............................... 2
Default Route Advertise..................... Disabled
Always...................................... FALSE
Metric.....................................
Metric Type................................. External Type 2
```

show ipv6 ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

Syntax

show ipv6 ospf abr

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf abr
Type  Router Id  Cost  Area ID   Next Hop                  Next Hop
                                                          Intf
----  --------  ----  --------  ----------------------    -----
INTRA  3.3.3.3   10    0.0.0.1   FE80::211:88FF:FE2A:3CB3  vlan11
INTRA  4.4.4.4   10    0.0.0.1   FE80::210:18FF:FE82:8E1   vlan12
```

show ipv6 ospf area

Use the **show ipv6 ospf area** command in Privileged EXEC mode to display information about the area.

Syntax

show ipv6 ospf area *areaid*

- *areaid*—Identifier for the OSPF area being displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about area 1.

```
console#show ipv6 ospf area 1

AreaID..................................... 0.0.0.1

External Routing........................... Import External
LSAs

Spf Runs................................... 0

Area Border Router Count.................... 0

Area LSA Count............................. 0

Area LSA Checksum.......................... 0

Stub Mode.................................. Disable

Import Summary LSAs........................ Enable
```

show ipv6 ospf asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR). This command takes no options.

Syntax

show ipv6 ospf asbr

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf asbr
Type   Router Id   Cost  Area ID   Next Hop                Next Hop
                                                            Intf
----   ---------   ----  --------  ----------------------  -------
INTRA  1.1.1.1     10    0.0.0.1   FE80::213:C4FF:FEDB:6C41  vlan10
INTRA  4.4.4.4      10    0.0.0.1   FE80::210:18FF:FE82:8E1   vlan12
```

show ipv6 ospf database

Use the **show ipv6 ospf database** command in Privileged EXEC mode to display information about the link state database when OSPFv3 is enabled. If no parameters are entered, the command displays the LSA headers. Optional parameters specify the type of link state advertisements to display.

The information below is only displayed if OSPF is enabled.

Syntax

show ipv6 ospf [*areaid*] **database** [{**external** | **inter-area** {**prefix** | **router**} | **link** | **network** | **nssa-external** | **prefix** | **router** | **unknown** [**area** | **as** | **link**]}] [*lsid*] [**adv-router** [*rtrid*] | **self-originate**]

- *areaid*—Identifies a specific OSPF area for which link state database information will be displayed.
- **external**—Displays the external LSAs.
- **inter-area**—Displays the inter-area LSAs.
- **link**—Displays the link LSAs.
- **network**—Displays the network LSAs.
- **nssa-external**—Displays NSSA external LSAs.
- **prefix**—Displays intra-area Prefix LSA.
- **router**—Displays router LSAs.

- **unknown**—Displays unknown area, AS or link-scope LSAs.
- *lsid*—Specifies a valid link state identifier (LSID).
- **adv-router**—Shows the LSAs that are restricted by the advertising router.
- *rtrid*—Specifies a valid router identifier.
- **self-originate**—Displays the LSAs in that are self originated.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the link state database when OSPFv3 is enabled.

```
console#show ipv6 ospf database

                Router Link States (Area 0.0.0.0)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
1.1.1.1                    0    4      80000034 54BD V6E--R- ----B
2.2.2.2                    0    2      80000044 95A5 V6E--R- ----B

                Network Link States (Area 0.0.0.0)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
2.2.2.2                  636    636   80000001 8B0D V6E--R-

                Inter Network States (Area 0.0.0.0)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------  --------------- ----- -------- ---- ------- -------
1.1.1.1                    1    323    80000001 3970
2.2.2.2                    1    322    80000001 1B8A
1.1.1.1                    2    293    80000001 3529
2.2.2.2                    2    375    80000001 FC5E
```

```
                Link States (Area 0.0.0.0)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
1.1.1.1                  634    700  80000008 2D89 V6E--R-
2.2.2.2                  634    689  8000000A 6F82 V6E--R-
2.2.2.2                  635    590  80000001 7782 V6E--R-


                Intra Prefix  States (Area 0.0.0.0)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
1.1.1.1                    0    1      8000003C 9F31
2.2.2.2                    0    2      8000004D 9126

                Router Link States (Area 0.0.0.1)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
1.1.1.1                    0    1      8000002E 35AD V6E--R- --V-B
2.2.2.2                    0    0      8000004A D2F3 V6E--R- ----B

                Network Link States (Area 0.0.0.1)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------  --------------- ----- -------- ---- ------- -------
1.1.1.1                  634   621    80000001 B9E2 V6E--R-

                Inter Network States (Area 0.0.0.1)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------  --------------- ----- -------- ---- ------- -------
1.1.1.1                  16    4      80000001 CA7C
2.2.2.2                  18    3      80000001 B28D
```

```
                Link States (Area 0.0.0.1)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
1.1.1.1                  634   441    80000003 B877 V6E--R-
2.2.2.2                  634   433    80000003 FE6E V6E--R-


                Intra Prefix  States (Area 0.0.0.1)
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
1.1.1.1                    0   6    8000003A 37C4
2.2.2.2                    0   1    8000004F 439A
1.1.1.1                10634   434  80000002 440A
```

show ipv6 ospf database database-summary

Use the **show ipv6 ospf database database-summary** command in Privileged EXEC mode to display the number of each type of LSA in the database and the total number of LSAs in the database.

Syntax

show ipv6 ospf database database-summary

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the number of each type of LSA in the database and the total number of LSAs in the database.

```
console#show ipv6 ospf database database-summary

OSPF Router with ID (0.0.0.2)
```

```
Router database summary
Router..................................... 0
Network.................................... 0
Inter-area Prefix.......................... 0
Inter-area Router.......................... 0
Type-7 Ext................................. 0
Link....................................... 0
Intra-area Prefix.......................... 0
Link Unknown............................... 0
Area Unknown............................... 0
AS Unknown................................. 0
Type-5 Ext................................. 0
Self-Originated Type-5 Ext................. 0
Total...................................... 0
```

show ipv6 ospf interface

Use the **show ipv6 ospf interface** command in Privileged EXEC mode to display the information for the IFO object or virtual interface tables.

Syntax

show ipv6 ospf interface {**vlan** *vlan-id*| **tunnel** *tunnel-id* | **loopback** *loopback-id*}

- *vlan-id*—Valid VLAN ID.
- *tunnel-id*—Tunnel identifier. (Range: 0-7)
- *loopback-id*—Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the information in VLAN 11's virtual interface tables.

```
console#show ipv6 ospf interface vlan 11
IP Address..................................... Err
ifIndex........................................ 1
OSPF Admin Mode................................ Enable
OSPF Area ID................................... 0.0.0.0
Router Priority................................ 1
Retransmit Interval............................ 5
Hello Interval................................. 10
Dead Interval.................................. 40
LSA Ack Interval............................... 1
Iftransit Delay Interval....................... 1
Authentication Type............................ None
Metric Cost.................................... 10 (computed)
OSPF Mtu-ignore................................ Disable
OSPF cannot be initialized on this interface.
```

show ipv6 ospf interface brief

Use the **show ipv6 ospf interface brief** command in Privileged EXEC mode to display brief information for the IFO object or virtual interface tables.

Syntax

show ipv6 ospf interface brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays brief ospf interface information.

```
console#show ipv6 ospf interface brief
                                        Hello Dead  Retrax       LSA
          Admin             Router      Int.  Int.  Int.  Retrax Ack
Interface Mode     Area ID  Prior. Cost Val.  Val.  Val.  Delay  Intval
--------- -------- --------  ------ ----- ----- ----- ------ ------ ------
```

show ipv6 ospf interface stats

Use the **show ipv6 ospf interface stats** command in User EXEC mode to display the statistics for a specific interface. The command only displays information if OSPF is enabled.

Syntax

show ipv6 ospf interface stats vlan *vlan-id*

- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the interface statistics for VLAN 5.

```
console>show  ipv6  ospf interface stats  vlan  5
OSPFv3 Area ID.............................. 0.0.0.1
Spf Runs.................................... 265
Area Border Router Count.................... 1
AS Border Router Count...................... 0
Area LSA Count.............................. 6
IPv6 Address.................................
FE80::202:BCFF:FE00:3146/1283FFE::2/64
OSPF Interface Events....................... 53
```

```
Virtual Events.............................. 13
Neighbor Events............................. 6
External LSA Count.......................... 0
LSAs Received............................... 660
Originate New LSAs.......................... 853
Sent Packets................................ 1013
Received Packets............................ 893
Discards.................................... 48
Bad Version................................. 0
Virtual Link Not Found...................... 9
Area Mismatch............................... 39
Invalid Destination Address................. 0
No Neighbor at Source Address............... 0
Invalid OSPF Packet Type.................... 0
  Packet Type             Sent      Received
--------------------      ----------  ----------
Hello                     295         219
Database Description      10          14
LS Request                4            4
LS Update                 521         398
LS Acknowledgement        209         282
```

show ipv6 ospf interface vlan

Use the **show ipv6 ospf interface vlan** command in Privileged EXEC mode to display OSPFv3 configuration and status information for a specific vlan.

Syntax

show ipv6 ospf interface vlan {*vlan-id*| **brief**}

- *vlan-id*—Valid VLAN ID. Range is 1-4093.
- **brief**—Displays a snapshot of configured interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays ospf interface vlan information.

```
console#show ipv6 ospf interface vlan 10
IPv6 Address..............................  FE80::2FC:E3FF:FE90:44
ifIndex...................................  634
OSPF Admin Mode...........................  Enable
OSPF Area ID..............................  0.0.0.1
Router Priority...........................  1
Retransmit Interval.......................  5
Hello Interval............................  10
Dead Interval.............................  40
LSA Ack Interval..........................  1
Iftransit Delay Interval..................  1
Authentication Type.......................  None
Metric Cost...............................  10  (computed)
OSPF Mtu-ignore...........................  Disable
OSPF Interface Type.......................  broadcast
State.....................................  backup-designated-router
Designated Router.........................  1.1.1.1
Backup Designated Router..................  2.2.2.2
Number of Link Events.....................  46
```

show ipv6 ospf neighbor

Use the **show ipv6 ospf neighbor** command in Privileged EXEC mode to display information about OSPF neighbors. If a neighbor IP address is not specified, the output displays summary information in a table. If an interface or tunnel is specified, only the information for that interface or tunnel displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Syntax

show ipv6 ospf neighbor [**interface** {**vlan** *vlan-id* | **tunnel** *tunnel-id*} [*ip-address*]

- *vlan-id*—Valid VLAN ID.
- *tunnel-id*—Tunnel identifier. (Range: 0-7)
- *ip-address*—Is the valid IP address of the neighbor about which information is displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display information about OSPF neighbors, in the first case in a summary table, and in the second in a table specific to tunnel 1.

```
console#show ipv6 ospf neighbor
Router ID Priority Intf Interface    State         Dead
                   ID                              Time
--------- -------- ---- -----------  ------------ ----

console#show ipv6 ospf neighbor interface tunnel 1
IP Address..................................... Err
ifIndex........................................ 619
OSPF Admin Mode................................ Enable
OSPF Area ID................................... 0.0.0.0
Router Priority................................ 1
```

```
Retransmit Interval.......................... 5
Hello Interval............................... 10
Dead Interval................................ 40
LSA Ack Interval............................. 1
Iftransit Delay Interval..................... 1
Authentication Type.......................... None
Metric Cost.................................. 1 (computed)
OSPF Mtu-ignore.............................. Disable
OSPF cannot be initialized on this interface.
```

show ipv6 ospf range

Use the **show ipv6 ospf range** command in Privileged EXEC mode to display information about the area ranges for the specified area identifier.

Syntax

show ipv6 ospf range *areaid*

- *areaid*—Identifies the OSPF area whose ranges are being displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the area ranges for area 1.

```
console#show ipv6 ospf range 1
Area ID   IPv6 Prefix/Prefix Length  Lsdb Type       Advertisement
--------- -------------------------  --------------- -------------
```

show ipv6 ospf stub table

Use the show ipv6 ospf stub table command in Privileged EXEC mode to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Syntax

show ipv6 ospf stub table

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
console#show ipv6 ospf stub table
AreaId       TypeofService   Metric Val   Import SummaryLSA
------------ -------------   ----------   -----------------
0.0.0.10         Normal       1             Enable
```

show ipv6 ospf virtual-link

Use the **show ipv6 ospf virtual-link** command in Privileged EXEC mode to display the OSPF Virtual Interface information for a specific area and neighbor.

Syntax

show ipv6 ospf virtual-link *areaid neighbor*

- *areaid*—Identifies the OSPF area whose virtual interface information is being displayed.
- *neighbor*—Router ID of neighbor.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information for area 1 and its neighbor.

```
console#show ipv6 ospf virtual-link 1 1.1.1.1
Area ID..................................... 1
Neighbor Router ID.......................... 1.1.1.1
Hello Interval.............................. 10
Dead Interval............................... 40
Iftransit Delay Interval.................... 1
Retransmit Interval......................... 5
State....................................... point-to-point
Metric...................................... 10
Neighbor State.............................. Full
```

show ipv6 ospf virtual-link brief

Use the **show ipv6 ospf virtual-link brief** command in Privileged EXEC mode to display the OSPFV3 Virtual Interface information for all areas in the system.

Syntax

show ipv6 ospf virtual-link brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
console(config)#show ipv6 ospf virtual-link brief
                        Hello      Dead       Retransmit Transit
Area ID     Neighbor    Interval   Interval   Interval   Delay
----------- ----------- ---------- ---------- ---------- --------
```

trapflags

Use the **trapflags** command in Router OSPFv3 Configuration mode to enable OSPF traps.

Syntax

trapflags

no trapflags

Default Configuration

Enabled is the default state.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF traps.

```
console(config)#ipv6 router ospf
console(config-rtr)#trapflags
```

52

PIM-DM Commands

ip pimdm

Use the **ip pimdm** command in Global Configuration mode to enable the administrative mode of PIM-DM in the router.

Syntax

ip pimdm

no ip pimdm

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables PIM-DM in the router.

```
console(config)#ip pimdm
```

ip pimdm mode

Use the **ip pimdm mode** command in Interface Configuration mode to set administrative mode of PIM-DM on an interface to enabled.

Syntax

ip pimdm mode

no ip pimdm mode

Default Configuration

Disabled is the default state.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets administrative mode of PIM-DM to enabled for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip pimdm mode
```

ip pimdm query-interval

Use the **ip pimdm query-interval** command in Interface Configuration mode to configure the transmission frequency of hello messages between PIM enabled neighbors.

Syntax

ip pimdm query-interval *seconds*

no ip pimdm query-interval

- *seconds*—Transmission frequency. (Range: 10-3600 seconds)

Default Configuration

30 seconds is the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the transmission frequency of hello messages at 50 seconds for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip pimdm query-interval 50
```

show ip pimdm

Use the **show ip pimdm** command in Privileged EXEC mode to display system-wide information for PIM-DM.

Syntax

show ip pimdm

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide information for PIM-DM.

```
console(config)#show ip pimdm
Admin Mode..................................... Disable
       PIM-DM INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
```

show ip pimdm interface

Use the **show ip pimdm interface** command in Privileged EXEC mode to display interface information for PIM-DM on the specified interface.

Syntax

show ip pimdm interface vlan *vlan-id*

- *vlan-id*—A valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example displays interface information for VLAN 11 PIM-DM.

```
console(config)#show ip pimdm interface vlan 11

Interface Mode............................... Disable

Hello Interval (secs)........................ 30
```

show ip pimdm interface stats

Use the **show ip pimdm interface stats** command in Privileged EXEC mode to display the statistical information for PIM-DM on the specified interface.

Syntax
show ip pimdm interface stats [**vlan** *vlan-id* | **all**]

- *vlan-id*—A valid VLAN ID

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example display the statistical information for PIM-DM on all interfaces.

```
console(config)#show ip pimdm interface stats all

                                      Hello      Designated
Interface  IP Address      Nbr Count Interval   Router
---------- --------------- --------- ---------- ---------------
```

show ip pimdm neighbor

Use the **show ip pimdm neighbor** command in Privileged EXEC mode to display the neighbor information for PIM-DM on the specified interface.

Syntax

show ip pimdm neighbor [**vlan** *vlan-id* | **all**]

- *vlan-id*—A valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example display the neighbor information for PIM-DM on all interfaces.

```
console(config)#show ip pimdm neighbor all

                            Up Time   Expiry Time

Neighbor Addr  Interface    hh:mm:ss  hh:mm:ss

-------------- ---------- --------- -----------
```

53

PIM-SM Commands

ip pimsm

Use the **ip pimsm** command in Global Configuration mode to set administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled.

Syntax

ip pimsm

no ip pimsm

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables PIM-SM on the router.

```
console(config)#ip pimsm
```

ip pimsm cbsrhashmasklength

Use the **ip pimsm cbsrhashmasklength** command in Interface Configuration mode to configure the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface. This hash mask length is used in the hash algorithm for selecting the RP for a particular group.

Syntax

ip pimsm cbsrhashmasklength *masklength*

no ip pimsm cbsrhashmasklength

- *masklength*—CBSR hash mask length. (Range: 0-32)

Default Configuration

30 is the default value for CBSR hash mask length.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a CBSR hash mask length of 5 for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip pimsm cbsrhashmasklength 5
```

ip pimsm cbsrpreference

Use the **ip pimsm cbsrpreference** command in Interface Configuration mode to configure the CBSR preference for a particular PIM-SM interface.

Syntax

ip pimsm cbsrpreference *preference*

no ip pimsm cbsrpreference

- *preference*—CBSR preference. (Range: 1-255)

Default Configuration

The default value for CBSR preference is 0.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the CBSR preference of 5 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip pimsm cbsrpreference 5
```

ip pimsm crppreference

Use the **ip pimsm crppreference** command in Interface Configuration mode to configure the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface. The active router interface, with the highest IP Address and crppreference greater than -1, is chosen as the CRP for the router. In the CRP advertisements sent to the bootstrap router (BSR), the router interface advertises itself as the CRP for the group range 224.0.0.0 mask 240.0.0.0.

Syntax

ip pimsm crppreference *preference*

no ip pimsm crppreference

preference—CPR preference. (Range: The valid values are from -1 to 255. The value of -1 is used to indicate that the local interface is not a Candidate RP interface.)

Default Configuration

0 is the default value for CPR preference.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a Candidate Rendezvous Point (CRP) of 5 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip pimsm crppreference 5
```

ip pimsm message-interval

Use the **ip pimsm message-interval** command in Global Configuration mode to configure the global join/prune interval for PIM-SM router.

Syntax

ip pimsm message-interval *interval*

no ip pimsm message-interval

- *interval*—Join/prune interval. (Range: 10-3600 seconds)

Default Configuration

60 is the default value for the join/prune interval.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a global join/prune interval for PIM-SM router of 100.

```
console(config)#ip pimsm message-interval 100
```

ip pimsm mode

Use the **ip pimsm mode** command in Interface Configuration mode to set to enabled the administrative mode of PIM-SM multicast routing on a routing interface.

Syntax

ip pimsm mode

no ip pimsm mode

Default Configuration

Disabled is the default state.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the administrative mode of PIM-SM multicast routing for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip pimsm mode
```

ip pimsm query-interval

Use the **ip pimsm query-interval** command in Interface Configuration mode to configure the transmission frequency of hello messages in seconds between PIM enabled neighbors.

Syntax

ip pimsm query-interval *seconds*

no ip pimsm query-interval

- *seconds*—Transmission frequency. (Range: 10-3600 seconds)

Default Configuration

30 seconds is the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the administrative mode of PIM-SM multicast routing for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip pimsm query-interval 50
```

ip pimsm register-rate-limit

Use the ip pimsm register-rate-limit command in Global Configuration mode to configure the Register Threshold rate for the RP (Rendezvous Point) router to switch to the shortest path. The rate is specified in Kilobits per second.

Syntax

ip pimsm register-rate-limit ***rate***

- *rate*—0-2000 kilobits per second

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration (VLAN) mode

User Guidelines

Use this command to control the number of register messages that the designated router (DR) will allow for each (S, G) entry.

When the value is set to zero, the PIM RP router joins the shortest path tree immediately after the first Register packet arrives from DR.

Example

```
console(config)#ip pimsm register-rate-limit 1000
```

ip pimsm spt-threshold

Use the **ip pimsm spt-threshold** command in Global Configuration mode to configure the Data Threshold rate for the last-hop (or leaf) router to switch to the shortest path. The rate is specified in kilobits per second.

Syntax

ip pimsm spt-threshold *threshold*

no ip pimsm spt-threshold

- *threshold*—Threshold rate. (Range: 0-2000 kilobits/sec)

Default Configuration

50 kilobits/sec is the default rate.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a threshold rate of 100 kilobits/sec.

```
console(config)#ip pimsm spt-threshold 100
```

ip pimsm staticrp

Use the **ip pimsm staticrp** command in Global Configuration mode to create RP IP address for the PIM-SM router.

Syntax

ip pimsm staticrp *ipaddr groupaddr groupmask*

no ip pimsm staticrp *ipaddr groupaddr groupmask*

- *ipaddr*—IP address of RP.
- *groupaddr*—Group IP address supported by RP.
- *groupmask*—Group subnet mask for group address.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example create RP IP address for the PIM-SM router.

```
console(config)#ip pimsm staticrp 10.1.1.1 224.5.5.5
255.255.255.255
```

ip pim-trapflags

Use the **ip pim-trapflags** command in Global Configuration mode to enable the PIM trap mode for both Sparse Mode (SM) and Dense Mode (DM).

Syntax

ip pim-trapflags

no ip pim-trapflags

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables PIM trap mode.

```
console(config)#ip pim-trapflags
```

show ip pimsm

Use the **show ip pimsm** command in Privileged EXEC mode to display the system-wide information for PIM-SM.

Syntax

show ip pimsm

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the system-wide information for PIM-SM.

```
console#show ip pimsm

Admin Mode..................................... Disable

Join/Prune Interval (secs)..................... 60

Data Threshold Rate (Kbps)..................... 50

Register Threshold Rate (Kbps)................. 50

        PIM-SM INTERFACE STATUS

Interface  Interface Mode  Protocol State

---------  --------------  --------------
```

show ip pimsm componenttable

Use the **show ip pimsm componenttable** command in Privileged EXEC mode to display the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

Syntax

show ip pimsm componenttable

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays objects specific to a PIM domain.

```
console#show ip pimsm componenttable

                  COMPONENT TABLE

Component   Component        Component        Component
Index BSR   Address BSR      Expiry Time      CRP Hold Time
                             (hh:mm:ss)       (hh:mm:ss)
----------  ---------------  ---------------  -------------
```

show ip pimsm interface

Use the **show ip pimsm interface** command in Privileged EXEC mode to display interface information for PIM-SM on the specified interface.

Syntax

show ip pimsm interface vlan *vlan-id*

- *vlan-id*—Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays interface information for VLAN 11 PIM-SM.

```
console#show ip pimsm interface vlan 11

Interface..................................... 11

IP Address.................................... 0.0.0.0

Subnet Mask................................... 0.0.0.0

Mode.......................................... Disable

Hello Interval (secs)......................... 30 secs

CBSR Preference............................... 0

CRP Preference................................ 0

CBSR Hash Mask Length......................... 30
```

show ip pimsm interface stats

Use the **show ip pimsm interface stats** command in User EXEC mode to display the statistical information for PIM-SM on the specified interface.

Syntax

show ip pimsm interface stats {**vlan** *vlan-id*|**all**}

- *vlan-id*—Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays statistical information for PIM-SM on all interfaces.

```
console> show ip pimsm interface stats all

                                    Designated Neighbor
Interface  IP Address      Mask     Router     Count
---------- --------------- -------- ---------- ---------------
```

show ip pimsm neighbor

Use the **show ip pimsm neighbor** command in Privileged EXEC mode to display neighbor information for PIM-SM on the specified interface.

Syntax

show ip pimsm neighbor [**vlan** *vlan-id*|**all**]

- *vlan-id*—Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays neighbor information for PIM-SM on all interfaces.

```
console#show ip pimsm neighbor all

                NEIGHBOR TABLE

Interface IP Address       Up Time    Expiry Time
                           (hh:mm:ss) (hh:mm:ss)
--------- ---------------- ---------- ------------
```

show ip pimsm rp

Use the **show ip pimsm rp** command in Privileged EXEC mode to display PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific group address or group mask provided in the command. The information in the table is displayed for each IP multicast group.

Syntax

show ip pimsm rp {*groupaddr groupmask* |**candidate**|**all**}

- *groupaddr* — Valid IP address.
- *groupmask* — Valid subnet mask.
- **all** — Enter "all" for all group addresses.

- candidate — Display PIM-SM candidate-RP table information.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups.

```
console#show ip pimsm rp all
                            RP SET TABLE
Group Address  Group Mask  Address  Hold Time Expiry Time Component
                                    (hh:mm:ss)(hh:mm:ss)
-------------  ----------  -------  --------- ----------- --------
```

show ip pimsm rphash

Use the **show ip pimsm rphash** command in Privileged EXEC mode to display the RP router being selected from the set of active RP routers. The RP router for the group is selected by using a hash algorithm.

Syntax

show ip pimsm rphash *groupaddr*

- *groupaddr*—Valid group IP address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the RP router being selected from the set of active RP routers.

```
console#show ip pimsm rphash 224.5.5.5

There are no static RPs for that group on the router.
```

show ip pimsm staticrp

Use the **show ip pimsm staticrp** command in Privileged EXEC mode to display the static RP information for the PIM-SM router.

Syntax

show ip pimsm staticrp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the static RP information for the PIM-SM router.

```
console#show ip pimsm staticrp

             STATIC RP TABLE

Address          Group Address      Group Mask

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

10.1.1.1           224.5.5.5         255.255.255.255
```

54

Router Discovery Protocol Commands

ip irdp

Use the **ip irdp** command in Interface Configuration mode to enable Router Discovery on an interface. Use the no form of the command to disable Router Discovery.

Syntax

ip irdp

no ip irdp

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables router discovery on the selected interface.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp
```

ip irdp address

Use the **ip irdp address** command in Interface Configuration mode to configure the address that the interface uses to send the router discovery advertisements. Use the no form of the command to return the address to the default.

Syntax

ip irdp address *ip-address*

no ip irdp address

- *ip-address*—IP address for router discovery advertisements. (Range: 224.0.0.1 [all-hosts IP multicast address] or 255.255.255.255 [limited broadcast address])

Default Configuration

IP address 224.0.0.1 is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the limited broadcast address as the IP address for router discovery advertisements.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip irdp address 255.255.255.255
```

ip irdp holdtime

Use the **ip irdp holdtime** command in Interface Configuration mode to configure the value, in seconds, of the holdtime field of the router advertisement sent from this interface. Use the no form of the command to set the time to the default value.

Syntax

ip irdp holdtime *integer*

no ip irdp holdtime

- *integer*—Integer value in seconds of the the holdtime field of the router advertisement sent from this interface. (Range: 600-9000 seconds)

Default Configuration

1800 seconds is the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets hold time at 2000 seconds for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip irdp holdtime 2000
```

ip irdp maxadvertinterval

Use the **ip irdp maxadvertinterval** command in Interface Configuration mode to configure the maximum time, in seconds, allowed between sending router advertisements from the interface. Use the no form of the command to set the time to the default value.

Syntax

ip irdp maxadvertinterval *integer*

no ip irdp maxadvertinterval

- *integer*—Maximum time in seconds allowed between sending router advertisements from the interface. (Range: 4 or the minimum advertisement interval, whichever is greater, and 1800 seconds)

Default Configuration

600 seconds is the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets maximum advertisement interval at 600 seconds for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip irdp maxadvertinterval 600
```

ip irdp minadvertinterval

Use the **ip irdp minadvertinterval** command in Interface Configuration mode to configure the minimum time, in seconds, allowed between sending router advertisements from the interface. Use the no form of the command to set the time to the default value.

Syntax

ip irdp minadvertinterval *integer*

no ip irdp minadvertinterval

- *integer*—Minimum time in seconds allowed between sending router advertisements from the interface. (Range: 3 to value of maximum advertisement interval in seconds)

Default Configuration

The minimum interval value is 450.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets minimum advertisement interval at 100 seconds for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip irdp minadvertinterval 100
```

ip irdp preference

Use the **ip irdp preference** command in Interface Configuration mode to configure the preference of the address as a default router address relative to other router addresses on the same subnet. Use the no form of the command to set the preference to the default value.

Syntax

ip irdp preference *integer*

no ip irdp preference

- *integer*—Preference of the address as a default router address, relative to other router addresses on the same subnet. (Range: -2147483648 to 2147483647)

Default Configuration

0 is the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the ip irdp preference to 1000 for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip irdp preference 1000
```

show ip irdp

Use the **show ip irdp** command in Privileged EXEC mode to display the router discovery information for all interfaces, or for a specified interface.

Syntax

show ip irdp {**vlan** *vlan-id* |**all**}

- *vlan-id*—Valid VLAN ID
- **all**—Shows information for all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows router discovery information for VLAN 15.

```
console#show ip irdp vlan 15

Interface  Ad Mode  Advertise Address Max Int Min Int Hold Time Preference

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

vlan15     Enable  224.0.0.1         600     450     1800     0
```

55

Routing Information Protocol (RIP) Commands

auto-summary

Use the **auto-summary** command in Router RIP Configuration mode to enable the RIP auto-summarization mode. Use the no form of the command to disable auto-summarization mode.

Syntax

auto-summary

no auto-summary

Default Configuration

Disabled is the default configuration.

Command Mode

Router RIP Configuration mode

User Guidelines

This command has no user guidelines.

Example

console(config-router)#auto-summary

default-information originate

Use the **default-information originate** command in Router RIP Configuration mode to control the advertisement of default routes.

Syntax

default-information originate

no default-information originate

Default Configuration

This command has no default configuration.

Command Mode

Router RIP Configuration mode

User Guidelines

This command has no user guidelines.

Example

console(config-router)#default-information originate

default-metric

Use the **default-metric** command in Router RIP Configuration mode to set a default for the metric of distributed routes. Use the no form of the command to return the metric to the default value.

Syntax

default-metric *integer*

no default-metric

- *integer*—Metric for the distributed routes. (Range: 1-15)

Default Configuration

Default metric is not configured by default.

Command Mode

Router RIP Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets a default of 12 for the metric of distributed routes.

```
console(config-router)#default-metric 12
```

distance rip

Use the **distance rip** command in Router RIP Configuration mode to set the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. Use the no form of the command to return the preference to the default value.

Syntax

distance rip *integer*

no distance rip

- *integer*—RIP route preference. (Range: 1-255)

Default Configuration

15 is the default configuration.

Command Mode

Router RIP Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the route preference value of RIP in the router at 100.

```
console(config-router)#distance rip 100
```

distribute-list out

Use the **distribute-list out** command in Router RIP Configuration mode to specify the access list to filter routes received from the source protocol. Use the no form of the command to remove the access list from the specified source protocol.

Syntax

distribute-list *accesslistname* **out {ospf | static | connected}**

no distribute-list *accesslistname* **out {ospf | static | connected}**

- *accesslistname*—The name used to identify the existing ACL. The range is 1-31 characters.
- **ospf**—Apply the specific access list when OSPF is the source protocol.
- **static**—Apply the specified access list when packets come through a static route.
- **connected**—Apply the specified access list when packets come from a directly connected route.

Default Configuration

This command has no default configuration.

Command Mode

Router RIP Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example elects access list ACL40 to filter routes received from the source protocol.

```
console(config-router)#distribute-list ACL40 out static
```

enable

Use the **enable** command in Router RIP Configuration mode to reset the default administrative mode of RIP in the router (active). Use the no form of the command to disable the administrative mode for RIP.

Syntax

enable

no enable

Default Configuration

Enabled is the default configuration.

Command Mode

Router RIP Configuration mode

User Guidelines

This command has no user guidelines.

Example

console(config-router)#enable

hostroutesaccept

Use the **hostroutesaccept** command in Router RIP Configuration mode to enable the RIP hostroutesaccept mode. Use the no form of the command to disable the RIP hostroutesaccept mode.

Syntax

hostroutesaccept

no hostroutesaccept

Default Configuration

Enabled is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

console(config-router)#hostroutesaccept

ip rip

Use the **ip rip** command in Interface Configuration mode to enable RIP on a router interface. Use the no form of the command to disable RIP on the interface.

Syntax

ip rip

no ip rip

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

console(config-if-vlan2)#ip rip

console(config-if-vlan2)#no ip rip

ip rip authentication

Use the **ip rip authentication** command in Interface Configuration Mode to set the RIP Version 2 Authentication Type and Key for the specified interface. Use the no form of the command to return the authentication to the default value.

Syntax

ip rip authentication {**none** | {**simple** *key*} | {**encrypt** *key key-id*}}

no ip rip authentication

- *key*—Authentication key for the specified interface. (Range: 16 bytes or less)
- **encrypt**—Specifies the Ethernet unit/port of the interface to view information.
- *key-id*—Authentication key identifier for authentication type encrypt. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the RIP Version 2 Authentication Type and Key for VLAN 11.

```
console(config-if-vlan11)#ip rip authentication encrypt pass123 35
```

ip rip receive version

Use the **ip rip receive version** command in Interface Configuration mode to configure the interface to allow RIP control packets of the specified version(s) to be received. Use the no form of the command to return the version to the default value.

Syntax

ip rip receive version {rip1 | rip2 | both | none}

no ip rip receive version

- **rip1**—Receive only RIP version 1 formatted packets.
- **rip2**—Receive only RIP version 2 formatted packets.
- **both**—Receive packets from either format.
- **none**—Do not allow any RIP control packets to be received.

Default Configuration

Both is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example allows no RIP control packets to be received by VLAN 11.

```
console(config-if-vlan11)#ip rip receive version none
```

ip rip send version

Use the **ip rip sent version** command in Interface Configuration mode to configure the interface to allow RIP control packets of the specified version to be sent. Use the no form of the command to return the version to the default value.

Syntax

ip rip send version {rip1 | rip1c | rip2 | none}

no ip rip send version

- **rip1**—Send RIP version 1 formatted packets.
- **rip1c**—Send RIP version 1 compatibility mode, which sends RIP version 2 formatted packets via broadcast.
- **rip2**—Send RIP version 2 using multicast.
- **none**—Do not allow any RIP control packets to be sent.

Default Configuration

RIP2 is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example allows no RIP control packets to be sent by VLAN 11.

```
console(config-if-vlan11)#ip rip send version none
```

redistribute

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. If the source protocol is OSPF, there are five possible match options.

Syntax

redistribute ospf [**metric** *integer*] [**match** [**internal**] [**external 1**] [**external 2**] [**nssa-external 1**] [**nssa-external 2**]]
no redistribute ospf

redistribute { **static** | **connected**} [**metric** *integer*]
no redistribute

- **metric** *integer*—Specifies the metric to use when redistributing the route. Range: 0-15.
- **match internal**—Adds internal matches to any match types presently being redistributed.
- **match external 1**—Adds routes imported into OSPF as Type-1 external routes into any match types presently being redistributed.
- **match external 2**—Adds routes imported into OSPF as Type-2 external routes into any match types presently being redistributed.
- **match nssa-external 1**—Adds routes imported into OSPF as NSSA Type-1 external routes into any match types presently being redistributed.
- **match nssa-external 2**—Adds routes imported into OSPF as NSSA Type-2 external routes into any match types presently being redistributed.
- **static**—Redistributes static routes.
- **connected**— Redistributes directly-connected routes.

Default Configuration

metric *integer*—not configured
match—internal

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-router)#redistribute ospf metric 10 match nssa-
external 1

console(config-router)#redistribute connected metric 1
```

router rip

Use the **router rip command** in Global Configuration mode to enter Router RIP mode.

Syntax

router rip

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters Router RIP mode.

```
console(config)#router rip
console(config-router)#
```

show ip rip

Use the **show ip** rip command in Privileged EXEC mode to display information relevant to the RIP router.

Syntax

show ip rip

Default Configuration

The command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information relevant to the RIP router.

```
console#show ip rip
RIP Admin Mode.............................. Enable
Split Horizon Mode.......................... Simple
Auto Summary Mode........................... Enable
Host Routes Accept Mode..................... Enable
```

```
Global route changes..................... 0
Global queries........................... 0
Default Metric........................... 12
Default Route Advertise.................. 0
Redistributing...........................
Source................................... Connected
Metric................................... 2
Distribute List.......................... Not configured
Redistributing...........................
Source................................... ospf
Metric................................... 10
Match Value.............................. 'nssa-external 1'
Distribute List.......................... Not configured
```

show ip rip interface

Use the **show ip rip interface** command in Privileged EXEC mode to display information related to a particular RIP interface.

Syntax

show ip rip interface vlan *vlan-id*

- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information related to the VLAN 15 RIP interface.

```
console#show ip rip interface vlan 15
```

```
Interface..................................... 15
IP Address.................................... -----
Send version.................................. RIP-2
Receive version............................... Both
RIP Admin Mode................................ Disable
Link State.................................... -----
Authentication Type........................... MD5
Authentication Key............................ "pass123"
Authentication Key ID......................... 35
Bad Packets Received.......................... -----
Bad Routes Received........................... -----
Updates Sent.................................. -----
```

show ip rip interface brief

Use the **show ip rip interface brief** command in Privileged EXEC mode to display general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

Syntax

show ip rip interface brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays general information for each RIP interface.

```
console#show ip rip interface brief

                         Send     Receive     RIP       Link
Interface  IP Address    Version  Version     Mode      State
```

```
---------- ----------    -------- ----------- --------- ----------
vlan1      0.0.0.0       RIP-2    Both        Disable   Down
vlan2      0.0.0.0       RIP-2    Both        Disable   Down
```

split-horizon

Use the **split-horizon** command in Router RIP Configuration mode to set the RIP split horizon mode. Use the no form of the command to return the mode to the default value.

Syntax

split-horizon {none | simple | poison}

no split-horizon

- **none**—RIP does not use split horizon to avoid routing loops.
- **simple**—RIP uses split horizon to avoid routing loops.
- **poison**—RIP uses split horizon with poison reverse (increases routing packet update size).

Default Configuration

Simple is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example does not use split horizon.

```
console(config-router)#split-horizon none
```

56

Tunnel Interface Commands

interface tunnel

Use the **interface tunnel** command in Global Configuration mode to enter the interface configuration mode for a tunnel.

Syntax

interface tunnel *tunnel-id*

no interface tunnel *tunnel-id*

- *tunnel-id*—Tunnel identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the interface configuration mode for tunnel 1.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#
```

show interfaces tunnel

Use the **show interfaces tunnel** command in Privileged EXEC mode to display the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Syntax

show interfaces tunnel [*tunnel-id*]

- *tunnel-id*—Tunnel identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples show the parameters related to an individual tunnel and to all tunnel interfaces.

```
console#show interfaces tunnel 1

Interface Link Status..........................  down

MTU size.....................................  1480 bytes


console#show interfaces tunnel

TunnelId    Interface      TunnelMode  SourceAddress   DestinationAddress

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

1           tunnel 1      IPv6OVER4   10.254.25.14    10.254.25.10

2           tunnel 2      IPv6OVER4                   10.254.20.10
```

tunnel destination

Use the **tunnel destination** command in Interface Configuration mode to specify the destination transport address of the tunnel.

Syntax

tunnel destination *ipv4addr*

no tunnel destination

- *ipv4addr*—Valid ipv4 address.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the destination transport address of tunnel 1.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel destination 10.1.1.1
```

tunnel mode ipv6ip

Use the **tunnel mode ipv6ip** command in Interface Configuration mode to specify the mode of the tunnel.

Syntax

tunnel mode ipv6ip

no tunnel mode ipv6ip

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies ipv6ip mode for tunnel 1.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel mode ipv6ip
```

tunnel source

Use the **tunnel source** command in Interface Configuration mode to specify the source transport address of the tunnel, either explicitly or by reference to an interface.

Syntax

tunnel source {*ipv4addr* | **vlan** *vlan-id*}

no tunnel source

- *ipv4addr*—Valid ipv4 address.
- *vlan-id*—Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies VLAN 11 as the source transport address of the tunnel.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel source vlan 11
```

57

Virtual LAN Routing Commands

show ip vlan

Use the **show ip vlan** command in Privileged EXEC mode to display the VLAN routing information for all VLANs with routing enabled.

Syntax

show ip vlan

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays VLAN routing information.

```
console#show ip vlan

MAC Address used by Routing VLANs: 00:00:00:01:00:02

VLAN ID IP Address      Subnet Mask

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

10      0.0.0.0         0.0.0.0

20      0.0.0.0         0.0.0.0
```

vlan routing

Use the **vlan routing** command in VLAN Database mode to create routing on a VLAN. Use the **no** form of the command to remove routing on the specified VLAN.

Syntax

vlan routing *vlan-id*

no vlan routing *vlan-id*

- *vlan-id*—VLAN identifier. (Range: 1-4093)

Default Configuration

Disabled is the default configuration.

Command Mode

VLAN Database mode

User Guidelines

This command has no user guidelines.

Example

The following example creates routing on VLAN 10.

```
console#vlan database
console(config-vlan)#vlan routing 10
```

58

Virtual Router Redundancy Protocol Commands

ip vrrp

Use the **ip vrrp** command in Global Configuration mode to enable the administrative mode of VRRP for the router. In Interface Config mode, this command enables the VRRP protocol on an interface. Use the **no** form of the command to disable the administrative mode of VRRP for the router.

Syntax (Global Config Mode)

ip vrrp

no ip vrrp

Syntax (Interface Config Mode)

ip vrrp *vr-id*

no ip vrrp *vr-id*

- vr-id—Virtual router identification. (Range: 1-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration or Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example in Global Configuration mode enables VRRP protocol on the router.

```
console(config)#ip vrrp
```

The following example in Interface Configuration mode enables VRRP protocol on VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip vrrp 5
```

ip vrrp authentication

Use the **ip vrrp authentication** command in Interface Configuration mode to set the authorization details value for the virtual router configured on a specified interface. Use the no form of the command to return the priority to the default value.

Syntax

ip vrrp *vr-id* **authentication** {**none** | **simple** *key*}

no ip vrrp *vr-id* **authentication**

- *vr-id*—The virtual router identifier. (Range: 1-255)
- **none**—Indicates authentication type is none.
- **simple**—Authentication type is a simple text password.
- *key*—The key for simple authentication. (Range: String values)

Default Configuration

None is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration mode sets the authorization details value for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip vrrp 5 authentication simple test123
```

ip vrrp ip

Use the **ip vrrp ip** command in Interface Configuration mode to set the virtual router IP address value for an interface. Use the **no** form of the command to remove the secondary IP address.

Syntax

ip vrrp *vr-id* **ip** *ip-address* [**secondary**]

no ip vrrp *vr-id* **ip** *ip-address* **secondary**

- *vr-id*—The virtual router identifier. (Range: 1-255)
- *ip-address*—The IP address of the virtual router.
- **secondary**—Designates the virtual router IP address as a secondary IP address on an interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The primary IP address can be modified, but not deleted. The **no** form of the command is only valid for the secondary IP address.

Example

The following example in Interface Configuration mode sets the virtual router IP address for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip vrrp 5 ip 192.168.5.25
```

ip vrrp mode

Use the **ip vrrp mode** command in Interface Configuration mode to enable the virtual router configured on an interface. Enabling the status field starts a virtual router. Use the no form of the command to disable the virtual router.

Syntax

ip vrrp *vr-id* **mode**

no ip vrrp *vr-id* **mode**

- *vr-id*—The virtual router identifier. (Range: 1-255)

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration mode enables the virtual router for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip vrrp 5 mode
```

ip vrrp preempt

Use the **ip vrrp preempt** command in Interface Configuration mode to set the preemption mode value for the virtual router configured on a specified interface. Use the **no** form of the command to disable preemption mode.

Syntax

ip vrrp *vr-id* **preempt**

no ip vrrp *vr-id* **preempt**

- *vr-id*—The virtual router identifier. (Range: 1-255)

Default Configuration

Enabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration mode sets the preemption mode value for the virtual router for VLAN 15.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ip vrrp 5 preempt
```

ip vrrp priority

Use the **ip vrrp priority** command in Interface Configuration mode to set the priority value for the virtual router configured on a specified interface. Use the no form of the command to return the priority to the default value.

Syntax

ip vrrp *vr-id* **priority** *priority*

no ip vrrp *vr-id* **priority**

- *vr-id*—The virtual router identifier. (Range: 1-255)
- *priority*—Priority value for the interface. (Range: 1-254)

Default Configuration

priority has a default value of 100.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration mode sets the priority value for the virtual router for VLAN 15.

```
console(config-if-vlan15)#ip vrrp 5 priority 20
```

ip vrrp timers advertise

Use the **ip vrrp timers advertise** command in Interface Configuration mode to set the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement. Use the no form of the command to return the advertisement frequency to the default value.

Syntax

ip vrrp *vr-id* **timers advertise** *seconds*

no ip vrrp *vr-id* **priority**

- *vr-id*—The virtual router identifier. (Range: 1-255)
- *seconds*—The frequency at which an interface on the specified virtual router sends a virtual router advertisement. (Range: 1-255 seconds)

Default Configuration

seconds has a default value of 1.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration mode sets the frequency at which the VLAN 15 virtual router sends a virtual router advertisement.

```
console(config-if-vlan15)#ip vrrp 5 timers advertise 10
```

show ip vrrp

Use the **show ip vrrp** command in Privileged EXEC mode to display whether VRRP functionality is enabled or disabled on the switch. The command also displays some global parameters which are required for monitoring.

Syntax

show ip vrrp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration displays VRRP's enabled status.

```
console#show ip vrrp

Admin Mode..................................... Enable

Router Checksum Errors......................... 0

Router Version Errors.......................... 0

Router VRID Errors............................. 0
```

show ip vrrp interface

Use the **show ip vrrp interface** command in Privileged EXEC mode to display all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Syntax

show ip vrrp interface vlan *vlan-id vr-id*

- *vlan-id*—Valid VLAN ID.
- *vr-id*—The virtual router identifier. (Range: 1-255)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example in Interface Configuration mode displays all configuration information about the VLAN 15 virtual router.

```
console#show ip vrrp interface vlan 15 5

Primary IP Address.............................. 192.168.5.55

VMAC Address.................................... 00:00:5e:00:01:05

Authentication Type............................. Simple

Priority........................................ 20

Advertisement Interval (secs)................... 10

Pre-empt Mode................................... Enable

Administrative Mode............................. Enable

State........................................... Initialized
```

show ip vrrp interface brief

Use the **show ip vrrp interface brief** command in Privileged EXEC mode to display information about each virtual router configured on the switch. It displays information about each virtual router.

Syntax

show ip vrrp interface brief

Default Configuration

This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example in Interface Configuration mode displays all configuration information about the virtual router on the selected interface.

```
console#show ip vrrp interface brief

Interface VRID IP Address     Mode    State

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

vlan1      2    0.0.0.0        Disable Initialize

vlan2      5    192.168.5.55   Enable  Initialize
```

show ip vrrp interface stats

Use the **show ip vrrp interface stats** command in User EXEC mode to display the statistical information about each virtual router configured on the switch.

Syntax
show ip vrrp interface stats vlan *vlan-id vr-id*

- *vlan-id*—Valid VLAN ID.
- *vr-id*—The virtual router identifier. (Range: 1-255)

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
This command has no user guidelines.

Example
The following example in Interface Configuration mode displays all statistical information about the VLAN 15 virtual router.

```
console>show ip vrrp interface stats vlan 15 5

UpTime.......................... 0 days 0 hrs 0 mins 0 secs
```

```
Protocol..................................... IP
State Transitioned to Master................. 0
Advertisement Received....................... 0
Advertisement Interval Errors................ 0
Authentication Failure....................... 0
IP TTL Errors................................ 0
Zero Priority Packets Received............... 0
Zero Priority Packets Sent................... 0
Invalid Type Packets Received................ 0
Address List Errors ......................... 0
Invalid Authentication Type.................. 0
Authentication Type Mismatch................. 0
Packet Length Errors......................... 0
```