



GEL-1061

10-Port L2 Managed Gigabit Switch, 2 x SFP

GEP-1061

**10-Port L2 Managed Gigabit PoE Switch, 2 x SFP,
802.3at PoE+, 125W**

GEL-2861

28-Port L2 Managed Gigabit Switch, 4 x SFP

CLI Reference Guide

V3.0

Digital Data Communications Asia Co., Ltd.

<http://www.level1.com>

CLI Reference Guide

GEL-1061

10-Port L2 Managed Gigabit Switch
with 8 10/100/1000BASE-T (RJ-45) Ports
and 2 Gigabit SFP Ports

GEP-1061

10-Port L2 Managed Gigabit PoE Switch
with 8 10/100/1000BASE-T (RJ-45) 802.3 af/at PoE Ports
and 2 Gigabit SFP Ports
(PoE Power Budget: 125 W)

GEL-2861 Managed Gigabit Switch

with 24 10/100/1000BASE-T (RJ-45) Ports
and 4 Gigabit SFP Ports

How to Use This Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read This Guide? This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized This guide describes the switch's command line interface (CLI). For more detailed information on the switch's key features or information about the web browser management interface refer to the *Web Management Guide*.

The guide includes these sections:

- ◆ Section I [“Getting Started”](#) — Includes information on initial configuration.
- ◆ Section II [“Command Line Interface”](#) — Includes all management options available through the CLI.
- ◆ Section III [“Appendices”](#) — Includes information on troubleshooting switch management access.

Related Documentation This guide focuses on switch software configuration through the CLI.

For information on how to manage the switch through the Web management interface, see the following guide:

User Manual

For information on how to install the switch, see the following guide:

Installation Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

Safety and Regulatory Information

Conventions The following conventions are used throughout this guide to show information:



Note: Emphasizes important information or calls your attention to related features or instructions.



Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

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

January 2022 Revision

This is the third version of this guide. This guide is valid for software release v1.2.2.9. It includes the following changes:

- ◆ Added "[Switch Clustering](#)" on page 152
- ◆ Added "[Flow Sampling Commands](#)" on page 193
- ◆ Added "[Web Authentication](#)" on page 276
- ◆ Added "[Configuring IEEE 802.1Q Tunneling](#)" on page 471
- ◆ Added "[IP Routing Commands](#)" on page 659
- ◆ Added "[Configuring MAC Based VLANs](#)" on page 480
- ◆ Added "[Multicast DNS Commands](#)" on page 605
- ◆ Updated "[Network Access \(MAC Address Authentication\)](#)" on page 265
- ◆ Updated "[DHCPv4 Snooping](#)" on page 282
- ◆ Updated "[Denial of Service Protection](#)" on page 314
- ◆ Updated "[Priority Commands \(Layer 3 and 4\)](#)" on page 494
- ◆ Updated "[File Management](#)" on page 100
- ◆ Updated "[Rate Limit Commands](#)" on page 413
- ◆ Updated "[Address Table Commands](#)" on page 425
- ◆ Updated "[Quality of Service Commands](#)" on page 501
- ◆ Removed GVRP

May 2016 Revision

This is the second version of this guide. This guide is valid for software release v1.1.2.0. It includes the following change:

- ◆ Added GEL-2861 model.

March 2016 Revision

This is the first version of this guide. This guide is valid for software release v1.1.2.0.

Contents

How to Use This Guide	3
Contents	7
Tables	33

Section I	Getting Started	39
1	Initial Switch Configuration	41
	Connecting to the Switch	41
	Configuration Options	41
	Connecting to the Console Port	42
	Logging Onto the Command Line Interface	43
	Setting Passwords	43
	Remote Connections	44
	Configuring the Switch for Remote Management	44
	Using the Network Interface	44
	Setting an IP Address	44
	Enabling SNMP Management Access	50
	Managing System Files	52
	Upgrading the Operation Code	53
	Saving or Restoring Configuration Settings	53
	Automatic Installation of Operation Code and Configuration Settings	55
	Downloading Operation Code from a File Server	55
	Specifying a DHCP Client Identifier	58
	Downloading a Configuration File and Other Parameters from a DHCP Server	59
	Setting the System Clock	61
	Setting the Time Manually	62
	Configuring SNTP	62
	Configuring NTP	63

Section II	Command Line Interface	65
2	Using the Command Line Interface	67
	Accessing the CLI	67
	Console Connection	67
	Telnet Connection	68
	Entering Commands	69
	Keywords and Arguments	69
	Minimum Abbreviation	69
	Command Completion	69
	Getting Help on Commands	70
	Partial Keyword Lookup	71
	Negating the Effect of Commands	72
	Using Command History	72
	Understanding Command Modes	72
	Exec Commands	72
	Configuration Commands	73
	Command Line Processing	75
	Showing Status Information	75
	CLI Command Groups	76
3	General Commands	79
	prompt	79
	reload (Global Configuration)	80
	enable	81
	quit	82
	show history	82
	configure	83
	disable	84
	reload (Privileged Exec)	84
	show reload	85
	end	85
	exit	85
4	System Management Commands	87

Device Designation	87
hostname	88
System Status	88
show access-list tcam-utilization	89
show memory	90
show process cpu	91
show process cpu guard	91
show process cpu task	92
show running-config	93
show startup-config	95
show system	95
show tech-support	96
show users	97
show version	98
show watchdog	99
watchdog software	99
Frame Size	99
jumbo frame	99
File Management	100
General Commands	102
boot system	102
copy	103
delete	107
dir	108
whichboot	109
Automatic Code Upgrade Commands	109
upgrade opcode auto	109
upgrade opcode path	110
upgrade opcode reload	111
show upgrade	112
TFTP Configuration Commands	112
ip tftp retry	112
ip tftp timeout	113
show ip tftp	113
Line	114

line	115
databits	115
exec-timeout	116
login	117
parity	118
password	118
password-thresh	119
silent-time	120
speed	121
stopbits	121
timeout login response	122
disconnect	122
terminal	123
show line	124
Event Logging	125
logging command	125
logging facility	126
logging history	126
logging host	127
logging on	128
logging trap	129
clear log	129
show log	130
show logging	131
SMTP Alerts	132
logging sendmail	133
logging sendmail destination-email	133
logging sendmail host	134
logging sendmail level	134
logging sendmail source-email	135
show logging sendmail	135
Time	136
SMTP Commands	137
smtp client	137
smtp poll	138

ntp server	138
show ntp	139
NTP Commands	140
ntp authenticate	140
ntp authentication-key	140
ntp client	141
ntp server	142
show ntp	143
Manual Configuration Commands	143
clock summer-time (date)	143
clock summer-time (predefined)	145
clock summer-time (recurring)	146
clock timezone	147
calendar set	148
show calendar	149
Time Range	149
time-range	149
absolute	150
periodic	151
show time-range	152
Switch Clustering	152
cluster	153
cluster commander	154
cluster ip-pool	155
cluster member	156
rcommand	156
show cluster	157
show cluster members	157
show cluster candidates	158
5 SNMP Commands	159
General SNMP Commands	161
snmp-server	161
snmp-server community	161
snmp-server contact	162

snmp-server location	162
show snmp	163
SNMP Target Host Commands	164
snmp-server enable traps	164
snmp-server host	165
snmp-server enable port-traps link-up-down	167
snmp-server enable port-traps mac-notification	168
show snmp-server enable port-traps	168
SNMPv3 Commands	169
snmp-server engine-id	169
snmp-server group	170
snmp-server user	171
snmp-server view	173
show snmp engine-id	174
show snmp group	175
show snmp user	176
show snmp view	177
Notification Log Commands	177
nlm	177
snmp-server notify-filter	178
show nlm oper-status	180
show snmp notify-filter	180
Additional Trap Commands	180
memory	180
process cpu	181
process cpu guard	182
6 Remote Monitoring Commands	185
rmon alarm	186
rmon event	187
rmon collection history	188
rmon collection rmon1	189
show rmon alarms	190
show rmon events	190
show rmon history	191

show rmon statistics	191
7 Flow Sampling Commands	193
sflow owner	193
sflow polling instance	195
sflow sampling instance	196
show sflow	197
8 Authentication Commands	199
User Accounts and Privilege Levels	200
enable password	200
username	201
privilege	203
show privilege	203
Authentication Sequence	204
authentication enable	204
authentication login	205
RADIUS Client	206
radius-server acct-port	206
radius-server auth-port	207
radius-server host	207
radius-server key	208
radius-server encrypted-key	209
radius-server retransmit	209
radius-server timeout	210
show radius-server	210
TACACS+ Client	211
tacacs-server host	211
tacacs-server key	212
tacacs-server encrypted-key	213
tacacs-server port	213
tacacs-server retransmit	214
tacacs-server timeout	214
show tacacs-server	215
AAA	215
aaa accounting commands	216

aaa accounting dot1x	217
aaa accounting exec	218
aaa accounting update	219
aaa authorization commands	219
aaa authorization exec	220
aaa group server	221
server	222
accounting dot1x	222
accounting commands	223
accounting exec	223
authorization commands	224
authorization exec	225
show accounting	225
show authorization	226
Web Server	227
ip http authentication	228
ip http port	228
ip http server	229
ip http secure-port	229
ip http secure-server	230
Telnet Server	231
ip telnet max-sessions	232
ip telnet port	232
ip telnet server	233
telnet (client)	233
show ip telnet	234
Secure Shell	234
ip ssh authentication-retries	237
ip ssh server	237
ip ssh server-key size	238
ip ssh timeout	239
delete public-key	239
ip ssh crypto host-key generate	240
ip ssh crypto zeroize	241
ip ssh save host-key	241

show ip ssh	242
show public-key	242
show ssh	243
802.1X Port Authentication	244
General Commands	244
dot1x default	244
dot1x system-auth-control	245
Authenticator Commands	246
dot1x intrusion-action	246
dot1x max-reauth-req	246
dot1x max-req	247
dot1x operation-mode	248
dot1x port-control	249
dot1x re-authentication	249
dot1x timeout quiet-period	250
dot1x timeout re-authperiod	250
dot1x timeout supp-timeout	251
dot1x timeout tx-period	251
dot1x re-authenticate	252
Information Display Commands	253
show dot1x	253
Management IP Filter	255
management	255
show management	256
9 General Security Measures	259
Port Security	260
mac-learning	260
port security	261
show port security	263
Network Access (MAC Address Authentication)	265
network-access aging	265
network-access mac-filter	266
mac-authentication reauth-time	267
network-access dynamic-qos	268

network-access dynamic-vlan	269
network-access guest-vlan	270
network-access max-mac-count	270
network-access mode mac-authentication	271
network-access port-mac-filter	272
mac-authentication intrusion-action	273
mac-authentication max-mac-count	273
clear network-access	274
show network-access	274
show network-access mac-address-table	275
show network-access mac-filter	276
Web Authentication	276
web-auth login-attempts	277
web-auth quiet-period	278
web-auth session-timeout	278
web-auth system-auth-control	279
web-auth	279
web-auth re-authenticate (Port)	280
web-auth re-authenticate (IP)	280
show web-auth	281
show web-auth interface	281
show web-auth summary	282
DHCPv4 Snooping	282
ip dhcp snooping	283
ip dhcp snooping information option	285
ip dhcp snooping information option encode no-subtype	286
ip dhcp snooping information option remote-id	288
ip dhcp snooping information option tr101 board-id	289
ip dhcp snooping information policy	289
ip dhcp snooping verify mac-address	290
ip dhcp snooping vlan	291
ip dhcp snooping information option circuit-id	292
ip dhcp snooping max-number	294
ip dhcp snooping trust	294
clear ip dhcp snooping binding	295

clear ip dhcp snooping database flash	295
ip dhcp snooping database flash	296
show ip dhcp snooping	296
show ip dhcp snooping binding	297
IPv4 Source Guard	297
ip source-guard binding	298
ip source-guard	300
ip source-guard max-binding	301
ip source-guard mode	302
clear ip source-guard binding blocked	303
show ip source-guard	303
show ip source-guard binding	304
ARP Inspection	305
ip arp inspection	306
ip arp inspection filter	307
ip arp inspection log-buffer logs	308
ip arp inspection validate	309
ip arp inspection vlan	310
ip arp inspection limit	311
ip arp inspection trust	311
show ip arp inspection configuration	312
show ip arp inspection interface	312
show ip arp inspection log	313
show ip arp inspection statistics	313
show ip arp inspection vlan	313
Denial of Service Protection	314
dos-protection echo-charge	314
dos-protection smurf	315
dos-protection tcp-flooding	315
dos-protection tcp-null-scan	316
dos-protection tcp-syn-fin-scan	316
dos-protection tcp-xmas-scan	317
dos-protection udp-flooding	317
dos-protection win-nuke	318
show dos-protection	318

Port-based Traffic Segmentation	319
traffic-segmentation	319
traffic-segmentation session	320
traffic-segmentation uplink/downlink	321
traffic-segmentation uplink-to-uplink	322
show traffic-segmentation	323
10 Access Control Lists	325
IPv4 ACLs	325
access-list ip	326
permit, deny (Standard IP ACL)	326
permit, deny (Extended IPv4 ACL)	327
ip access-group	330
show ip access-group	331
show ip access-list	331
IPv6 ACLs	332
access-list ipv6	332
permit, deny (Standard IPv6 ACL)	333
permit, deny (Extended IPv6 ACL)	334
ipv6 access-group	337
show ipv6 access-group	337
show ipv6 access-list	338
MAC ACLs	338
access-list mac	339
permit, deny (MAC ACL)	340
mac access-group	342
show mac access-group	343
show mac access-list	343
ARP ACLs	344
access-list arp	344
permit, deny (ARP ACL)	345
show access-list arp	346
ACL Information	347
clear access-list hardware counters	347
show access-group	347

show access-list	348
11 Interface Commands	349
Interface Configuration	350
interface	350
capabilities	351
description	352
flowcontrol	353
history	354
media-type	354
negotiation	355
shutdown	356
speed-duplex	356
clear counters	357
show interfaces brief	358
show interfaces counters	359
show interfaces history	363
show interfaces status	364
show interfaces switchport	365
Transceiver Threshold Configuration	367
transceiver-monitor	367
transceiver-threshold-auto	368
transceiver-threshold current	368
transceiver-threshold rx-power	369
transceiver-threshold temperature	370
transceiver-threshold tx-power	371
transceiver-threshold voltage	372
show interfaces transceiver	373
show interfaces transceiver-threshold	374
Cable Diagnostics	375
test cable-diagnostics	375
show cable-diagnostics	376
Power Savings	377
power-save	377
show power-save	378

12 Link Aggregation Commands	379
Manual Configuration Commands	380
port channel load-balance	380
channel-group	382
Dynamic Configuration Commands	383
lacp	383
lacp admin-key (Ethernet Interface)	384
lacp port-priority	385
lacp system-priority	386
lacp admin-key (Port Channel)	387
lacp timeout	388
Trunk Status Display Commands	389
show lacp	389
show port-channel load-balance	392
13 Power over Ethernet Commands	393
power inline compatible	393
power inline maximum allocation mode	394
power mainpower maximum allocation	395
power inline	396
power inline maximum allocation	396
power inline priority	397
power inline time-range	398
show power inline status	399
show power inline time-range	400
show power mainpower	401
14 Port Mirroring Commands	403
Local Port Mirroring Commands	403
port monitor	403
show port monitor	404
RSPAN Mirroring Commands	405
rspan source	407
rspan destination	408
rspan remote vlan	409
no rspan session	410

show rspan	411
15 Congestion Control Commands	413
Rate Limit Commands	413
rate-limit	414
Storm Control Commands	416
switchport packet-rate	416
16 Loopback Detection Commands	419
loopback-detection	420
loopback-detection action	420
loopback-detection recover-time	421
loopback-detection transmit-interval	422
loopback detection trap	422
loopback-detection release	423
show loopback-detection	423
17 Address Table Commands	425
mac-address-table aging-time	425
mac-address-table static	426
clear mac-address-table dynamic	427
show mac-address-table	428
show mac-address-table aging-time	429
show mac-address-table count	429
18 Spanning Tree Commands	431
spanning-tree	432
spanning-tree cisco-prestandard	433
spanning-tree forward-time	433
spanning-tree hello-time	434
spanning-tree max-age	435
spanning-tree mode	435
spanning-tree mst configuration	437
spanning-tree pathcost method	437
spanning-tree priority	438
spanning-tree system-bpdu-flooding	439
spanning-tree transmission-limit	439

max-hops	440
mst priority	441
mst vlan	441
name	442
revision	443
spanning-tree bpdu-filter	443
spanning-tree bpdu-guard	444
spanning-tree cost	445
spanning-tree edge-port	447
spanning-tree link-type	448
spanning-tree loopback-detection	448
spanning-tree loopback-detection action	449
spanning-tree loopback-detection release-mode	450
spanning-tree loopback-detection trap	451
spanning-tree mst cost	451
spanning-tree mst port-priority	452
spanning-tree port-bpdu-flooding	453
spanning-tree port-priority	453
spanning-tree root-guard	454
spanning-tree spanning-disabled	455
spanning-tree tc-prop-stop	455
spanning-tree loopback-detection release	456
spanning-tree protocol-migration	457
show spanning-tree	457
show spanning-tree mst configuration	460
19 VLAN Commands	461
Editing VLAN Groups	461
vlan database	462
vlan	462
Configuring VLAN Interfaces	463
interface vlan	464
switchport acceptable-frame-types	465
switchport allowed vlan	465
switchport forbidden vlan	467

switchport ingress-filtering	467
switchport mode	468
switchport native vlan	469
Displaying VLAN Information	470
show vlan	470
Configuring IEEE 802.1Q Tunneling	471
dot1q-tunnel system-tunnel-control	472
dot1q-tunnel tpid	473
switchport dot1q-tunnel mode	474
switchport dot1q-tunnel priority map	474
show dot1q-tunnel	475
Configuring Protocol-based VLANs	476
protocol-vlan protocol-group (Configuring Groups)	477
protocol-vlan protocol-group (Configuring Interfaces)	477
show protocol-vlan protocol-group	478
show interfaces protocol-vlan protocol-group	479
Configuring MAC Based VLANs	480
mac-vlan	480
show mac-vlan	481
Configuring Voice VLANs	482
voice vlan	482
voice vlan aging	483
voice vlan mac-address	484
switchport voice vlan	485
switchport voice vlan priority	486
switchport voice vlan rule	486
switchport voice vlan security	487
show voice vlan	488
20 Class of Service Commands	489
Priority Commands (Layer 2)	489
queue mode	490
queue weight	491
switchport priority default	492
show queue mode	493

show queue weight	493
Priority Commands (Layer 3 and 4)	494
qos map cos-queue	494
qos map dscp-queue	496
qos map trust-mode	497
show qos map cos-queue	498
show qos map dscp-queue	499
show qos map trust-mode	499
21 Quality of Service Commands	501
class-map	502
description	503
match	504
rename	505
policy-map	505
class	506
police rate	507
set cos	508
set ip dscp	509
service-policy	509
show class-map	510
show policy-map	511
show policy-map interface	511
22 Multicast Filtering Commands	513
IGMP Snooping	514
ip igmp snooping	515
ip igmp snooping proxy-reporting	516
ip igmp snooping querier	516
ip igmp snooping router-alert-option-check	517
ip igmp snooping router-port-expire-time	517
ip igmp snooping tcn-flood	518
ip igmp snooping tcn-query-solicit	519
ip igmp snooping unregistered-data-flood	520
ip igmp snooping unsolicited-report-interval	520
ip igmp snooping version	521

ip igmp snooping version-exclusive	522
ip igmp snooping vlan general-query-suppression	522
ip igmp snooping vlan immediate-leave	523
ip igmp snooping vlan last-memb-query-count	524
ip igmp snooping vlan last-memb-query-intvl	525
ip igmp snooping vlan mrd	525
ip igmp snooping vlan proxy-address	526
ip igmp snooping vlan query-interval	528
ip igmp snooping vlan query-resp-intvl	528
ip igmp snooping vlan static	529
clear ip igmp snooping groups dynamic	530
clear ip igmp snooping statistics	530
show ip igmp snooping	531
show ip igmp snooping group	532
show ip igmp snooping mrouter	533
show ip igmp snooping statistics	533
Static Multicast Routing	536
ip igmp snooping vlan mrouter	536
IGMP Filtering and Throttling	537
ip igmp filter (Global Configuration)	538
ip igmp profile	538
permit, deny	539
range	539
ip igmp filter (Interface Configuration)	540
ip igmp max-groups	541
ip igmp max-groups action	541
ip igmp query-drop	542
show ip igmp filter	543
show ip igmp profile	543
show ip igmp query-drop	544
show ip igmp throttle interface	545
MLD Snooping	546
ipv6 mld snooping	547
ipv6 mld snooping proxy-reporting	547
ipv6 mld snooping querier	548

ipv6 mld snooping query-interval	549
ipv6 mld snooping query-max-response-time	549
ipv6 mld snooping robustness	550
ipv6 mld snooping router-port-expire-time	550
ipv6 mld snooping unknown-multicast mode	551
ipv6 mld snooping unsolicited-report-interval	552
ipv6 mld snooping version	552
ipv6 mld snooping vlan immediate-leave	553
ipv6 mld snooping vlan mrouter	553
ipv6 mld snooping vlan static	554
clear ipv6 mld snooping groups dynamic	555
clear ipv6 mld snooping statistics	555
show ipv6 mld snooping	556
show ipv6 mld snooping group	556
show ipv6 mld snooping mrouter	559
show ipv6 mld snooping statistics	559
MLD Filtering and Throttling	563
ipv6 mld filter (Global Configuration)	564
ipv6 mld profile	565
permit, deny	565
range	566
ipv6 mld filter (Interface Configuration)	567
ipv6 mld max-groups	567
ipv6 mld max-groups action	568
ipv6 mld query-drop	569
show ipv6 mld filter	569
show ipv6 mld profile	570
show ipv6 mld query-drop	570
show ipv6 mld throttle interface	572
23 LLDP Commands	573
lldp	575
lldp holdtime-multiplier	575
lldp med-fast-start-count	576
lldp notification-interval	576

lldp refresh-interval	577
lldp reinit-delay	577
lldp tx-delay	578
lldp admin-status	579
lldp basic-tlv management-ip-address	579
lldp basic-tlv port-description	580
lldp basic-tlv system-capabilities	580
lldp basic-tlv system-description	581
lldp basic-tlv system-name	581
lldp dot1-tlv proto-ident	582
lldp dot1-tlv proto-vid	582
lldp dot1-tlv pvid	583
lldp dot1-tlv vlan-name	583
lldp dot3-tlv link-agg	584
lldp dot3-tlv mac-phy	584
lldp dot3-tlv max-frame	585
lldp dot3-tlv poe	585
lldp med-location civic-addr	586
lldp med-notification	588
lldp med-tlv ext-poe	588
lldp med-tlv inventory	589
lldp med-tlv location	589
lldp med-tlv med-cap	590
lldp med-tlv network-policy	590
lldp notification	591
show lldp config	592
show lldp info local-device	593
show lldp info remote-device	594
show lldp info statistics	596
24 Domain Name Service Commands	597
DNS Commands	598
ip domain-list	598
ip domain-lookup	599
ip domain-name	600

ip host	600
ip name-server	601
ipv6 host	602
clear dns cache	603
clear host	603
show dns	604
show dns cache	604
show hosts	605
Multicast DNS Commands	605
ip mdns	605
show ip mdns	606
25 DHCP Commands (IPv4 and IPv6)	607
DHCP Client	607
DHCP for IPv4	608
ip dhcp dynamic-provision	608
ip dhcp client class-id	609
ip dhcp restart client	611
show ip dhcp dynamic-provision	611
DHCP for IPv6	612
ipv6 dhcp client rapid-commit vlan	612
ipv6 dhcp restart client vlan	612
show ipv6 dhcp duid	614
show ipv6 dhcp vlan	614
DHCP Relay (IPv4 and IPv6)	615
ip dhcp relay server	615
ip dhcp restart relay	616
ipv6 dhcp relay destination	617
ipv6 dhcp relay destination multicast	618
show ipv6 dhcp relay destination interface	619
26 IP Interface Commands	621
IPv4 Interface	621
Basic IPv4 Configuration	622
ip address	622
ip default-gateway	624

show ip interface	625
show ip traffic	625
traceroute	626
ping	627
ip multicast-data-drop	628
show ip multicast-data-drop	629
ARP Configuration	630
arp	630
ip proxy-arp	631
clear arp-cache	632
show arp	632
IPv6 Interface	633
Interface Address Configuration and Utilities	634
ipv6 default-gateway	634
ipv6 address	635
ipv6 address autoconfig	636
ipv6 address eui-64	638
ipv6 address link-local	640
ipv6 enable	641
ipv6 mtu	642
show ipv6 default-gateway	643
show ipv6 interface	643
show ipv6 mtu	645
show ipv6 traffic	646
clear ipv6 traffic	650
ping6	651
traceroute6	652
Neighbor Discovery	653
ipv6 nd dad attempts	653
ipv6 nd ns-interval	655
ipv6 nd reachable-time	656
clear ipv6 neighbors	656
show ipv6 neighbors	657
28 IP Routing Commands	659

Global Routing Configuration	659
IPv4 Commands	660
ip route	660
show ip route	661
Routing Information Protocol (RIP)	662
router rip	663
default-information originate	664
default-metric	664
distance	665
maximum-prefix	666
neighbor	667
network	667
passive-interface	668
redistribute	669
timers basic	670
version	671
ip rip authentication mode	672
ip rip authentication string	673
ip rip receive version	673
ip rip receive-packet	674
ip rip send version	675
ip rip send-packet	676
ip rip split-horizon	676
clear ip rip route	677
clear ip rip statistics	678
show ip protocols rip	679
show ip rip	679

Section III	Appendices	681
	A Troubleshooting	683
	Problems Accessing the Management Interface	683
	Using System Logs	684
	B License Information	685

The GNU General Public License	685
Glossary	689
List of CLI Commands	697

Tables

Table 1: Options 60, 66 and 67 Statements	60
Table 2: Options 55 and 124 Statements	60
Table 3: General Command Modes	72
Table 4: Configuration Command Modes	74
Table 5: Keystroke Commands	75
Table 6: Command Group Index	76
Table 7: General Commands	79
Table 8: System Management Commands	87
Table 9: Device Designation Commands	87
Table 10: System Status Commands	88
Table 11: show access-list tcam-utilization - display description	90
Table 12: show process cpu guard - display description	92
Table 13: show system – display description	96
Table 14: show version – display description	98
Table 15: Frame Size Commands	99
Table 16: Flash/File Commands	101
Table 17: File Directory Information	108
Table 18: Line Commands	114
Table 19: Event Logging Commands	125
Table 20: Logging Levels	127
Table 21: show logging flash/ram - display description	131
Table 22: show logging trap - display description	132
Table 23: Event Logging Sendmail Commands	132
Table 24: Time Commands	136
Table 25: Predefined Summer-Time Parameters	145
Table 26: Time Range Commands	149
Table 27: Switch Cluster Commands	152
Table 28: SNMP Commands	159
Table 29: show snmp engine-id - display description	174

Table 30: show snmp group - display description	175
Table 31: show snmp user - display description	176
Table 32: show snmp view - display description	177
Table 33: RMON Commands	185
Table 34: sFlow Commands	193
Table 35: Authentication Commands	199
Table 36: User Access Commands	200
Table 37: Default Login Settings	202
Table 38: Authentication Sequence Commands	204
Table 39: RADIUS Client Commands	206
Table 40: TACACS+ Client Commands	211
Table 41: AAA Commands	215
Table 42: Web Server Commands	227
Table 43: HTTPS System Support	231
Table 44: Telnet Server Commands	231
Table 45: Secure Shell Commands	234
Table 46: show ssh - display description	243
Table 47: 802.1X Port Authentication Commands	244
Table 48: Management IP Filter Commands	255
Table 49: General Security Commands	259
Table 50: Management IP Filter Commands	260
Table 51: show port security - display description	263
Table 52: Network Access Commands	265
Table 53: Dynamic QoS Profiles	268
Table 54: Web Authentication	277
Table 55: DHCP Snooping Commands	282
Table 56: Option 82 information	287
Table 57: Option 82 information	292
Table 58: IPv4 Source Guard Commands	297
Table 59: ARP Inspection Commands	305
Table 60: DoS Protection Commands	314
Table 61: Commands for Configuring Traffic Segmentation	319
Table 62: Traffic Segmentation Forwarding	320
Table 63: Access Control List Commands	325
Table 64: IPv4 ACL Commands	325

Table 65: IPv6 ACL Commands	332
Table 66: MAC ACL Commands	338
Table 67: ARP ACL Commands	344
Table 68: ACL Information Commands	347
Table 69: Interface Commands	349
Table 70: show interfaces counters - display description	360
Table 71: show interfaces switchport - display description	366
Table 72: Link Aggregation Commands	379
Table 73: show lacp counters - display description	389
Table 74: show lacp internal - display description	390
Table 75: show lacp neighbors - display description	391
Table 76: show lacp sysid - display description	392
Table 77: PoE Commands	393
Table 78: Maximum PoE Based on PD Classification	395
Table 79: Maximum Number of Ports Providing Simultaneous Power	397
Table 80: show power inline status - display description	400
Table 81: show power mainpower - display description	401
Table 82: Port Mirroring Commands	403
Table 83: Mirror Port Commands	403
Table 84: RSPAN Commands	405
Table 85: Congestion Control Commands	413
Table 86: Rate Limit Commands	413
Table 87: Rate Limit Commands	416
Table 88: Loopback Detection Commands	419
Table 89: Address Table Commands	425
Table 90: Spanning Tree Commands	431
Table 91: Recommended STA Path Cost Range	445
Table 92: Default STA Path Costs	446
Table 93: VLAN Commands	461
Table 94: Commands for Editing VLAN Groups	461
Table 95: Commands for Configuring VLAN Interfaces	463
Table 96: Commands for Displaying VLAN Information	470
Table 97: 802.1Q Tunneling Commands	471
Table 98: Protocol-based VLAN Commands	476
Table 99: MAC Based VLAN Commands	480

Table 100: Voice VLAN Commands	482
Table 101: Priority Commands	489
Table 102: Priority Commands (Layer 2)	489
Table 103: Priority Commands (Layer 3 and 4)	494
Table 104: Default Mapping of CoS/CFI Values to Queue/CFI	495
Table 105: Default Mapping of DSCP Values to Queue	496
Table 106: Quality of Service Commands	501
Table 107: Multicast Filtering Commands	513
Table 108: IGMP Snooping Commands	514
Table 109: show ip igmp snooping statistics input - display description	534
Table 110: show ip igmp snooping statistics output - display description	535
Table 111: show ip igmp snooping statistics vlan query - display description	535
Table 112: Static Multicast Interface Commands	536
Table 113: IGMP Filtering and Throttling Commands	537
Table 114: MLD Snooping Commands	546
Table 115: show ipv6 MLD snooping statistics input - display description	560
Table 116: show ipv6 MLD snooping statistics output - display description	561
Table 117: show ipv6 MLD snooping statistics query - display description	561
Table 118: show ipv6 MLD snooping statistics summary - display description	562
Table 119: MLD Filtering and Throttling Commands	563
Table 120: LLDP Commands	573
Table 121: LLDP MED Location CA Types	587
Table 122: Address Table Commands	597
Table 123: show dns cache - display description	604
Table 124: show hosts - display description	605
Table 125: DHCP Commands	607
Table 126: DHCP Client Commands	607
Table 127: Options 60, 66 and 67 Statements	610
Table 128: Options 55 and 124 Statements	610
Table 129: DHCP Relay Commands	615
Table 130: IP Interface Commands	621
Table 131: IPv4 Interface Commands	621
Table 132: Basic IP Configuration Commands	622
Table 133: Address Resolution Protocol Commands	630
Table 134: IPv6 Configuration Commands	633

Table 135: show ipv6 interface - display description	644
Table 136: show ipv6 mtu - display description	646
Table 137: show ipv6 traffic - display description	647
Table 138: show ipv6 neighbors - display description	657
Table 160: IP Routing Commands	659
Table 161: Global Routing Configuration Commands	659
Table 162: Routing Information Protocol Commands	662
Table 163: Troubleshooting Chart	683

Section I

Getting Started

This section describes how to configure the switch for management access through the web interface or SNMP.

This section includes these chapters:

- ◆ ["Initial Switch Configuration" on page 41](#)

1

Initial Switch Configuration

This chapter includes information on connecting to the switch and basic configuration procedures.

Connecting to the Switch

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).



Note: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see [“Setting an IP Address” on page 44](#).

Configuration Options

The switch’s HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 9, Mozilla Firefox 39, or Google Chrome 44, or more recent versions. The switch’s web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software.

The switch’s web interface, console interface, and SNMP agent allow you to perform the following management functions:

- ◆ Set user names and passwords
- ◆ Set an IP interface for any VLAN
- ◆ Configure SNMP parameters
- ◆ Enable/disable any port
- ◆ Set the speed/duplex mode for any port
- ◆ Configure the bandwidth of any port by limiting input or output rates
- ◆ Control port access through IEEE 802.1X security or static address filtering

- ◆ Filter packets using Access Control Lists (ACLs)
- ◆ Configure up to 4094 IEEE 802.1Q VLANs
- ◆ Configure IP routing for unicast traffic
- ◆ Configure IGMP multicast filtering
- ◆ Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/SFTP/TFTP (using the command line or web interface)
- ◆ Configure Spanning Tree parameters
- ◆ Configure Class of Service (CoS) priority queuing
- ◆ Configure static or LACP trunks (up to 8)
- ◆ Enable port mirroring
- ◆ Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- ◆ Display system information and statistics

Connecting to the Console Port

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the R-45 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
 - Select the appropriate serial port (COM port 1 or COM port 2).
 - Set the baud rate to 115200 bps.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set flow control to none.
 - Set the emulation mode to VT100.
 - When using HyperTerminal, select Terminal keys, not Windows keys.

4. Power on the switch.

After the system completes the boot cycle, the logon screen appears.

Logging Onto the Command Line Interface

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the User Name prompt, enter “admin.”
3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 32 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:
```

```
CLI session with the GEL-2861* is opened.
To end the CLI session, enter [Exit].
```

```
Console#configure
Console(config)#username guest password 0 [password]
```

```
Console(config)#username admin password 0 [password]  
Console(config)#
```

- * This manual covers the GEL-2861 and GEL-1061 Gigabit Ethernet switches. Other than the difference in port types, and support for PoE, there are no significant differences.

Remote Connections Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IPv4 or IPv6 address, subnet mask, and default gateway using a console connection, BOOTP or DHCP protocol. To configure this device as the default gateway, use the [ip default-gateway](#) command.

An IPv4 address for the switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see ["Setting an IP Address" on page 44](#).

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet or SSH from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions), or from a network computer using SNMP network management software.



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

Note: Any VLAN group can be assigned an IP interface address ([page 44](#)) for managing the switch.

The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Configuring the Switch for Remote Management

Using the Network Interface The switch can be managed through the operational network, known as in-band management. Because in-band management traffic is mixed in with operational network traffic, it is subject to all of the filtering rules usually applied to a standard network ports such as ACLs and VLAN tagging. In-band network management can be accessed via a connection to any network port (1-10/28).

Setting an IP Address You must establish IP address information for a switch to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router. To configure this device as the default gateway, use the `ip default-gateway` command.

- ◆ **Dynamic** — The switch can send IPv4 configuration requests to BOOTP or DHCP address allocation servers on the network, or automatically generate a unique IPv6 host address based on the local subnet address prefix received in router advertisement messages. An IPv6 link local address for use in a local network can also be dynamically generated as described in [“Obtaining an IPv6 Address” on page 49](#).

This switch is designed as a router, and therefore does not support DHCP for IPv6, so an IPv6 global unicast address for use in a network containing more than one subnet can only be manually configured as described in [“Assigning an IPv6 Address” on page 46](#).

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.



Note: The default IPv4 address and subnet mask for VLAN 1 is 192.168.2.10 255.255.255.255, with no defined default gateway.

Assigning an IPv4 Address

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- ◆ IP address for the switch
- ◆ Network mask for this network
- ◆ Default gateway for the network

To assign an IPv4 address to the switch, complete the following steps

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
```

Assigning an IPv6 Address

This section describes how to configure a “link local” address for connectivity within the local subnet only, and also how to configure a “global unicast” address, including a network prefix for use on a multi-segment network and the host portion of the address.

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see [“IPv6 Interface” on page 633](#).

Link Local Address — All link-local addresses must be configured with a prefix in the range of FE80~FEBF. Remember that this address type makes the switch accessible over IPv6 for all devices attached to the same local subnet only. Also, if the switch detects that the address you configured conflicts with that in use by another device on the subnet, it will stop using the address in question, and automatically generate a link local address that does not conflict with any other devices on the local subnet.

To configure an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ipv6 address” followed by up to 8 colon-separated 16-bit hexadecimal values for the *ipv6-address* similar to that shown in the example, followed by the “link-local” command parameter. Then press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
(None)
Joined group address(es):
ff02::1:ff11:6700
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
```

```
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

```
Console#
```

Address for Multi-segment Network — Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

- ◆ Prefix for this network
- ◆ IP address for the switch
- ◆ Default gateway for the network

For networks that encompass several different subnets, you must define the full address, including a network prefix and the host address for the switch. You can specify either the full IPv6 address, or the IPv6 address and prefix length. The prefix length for an IPv6 network is the number of bits (from the left) of the prefix that form the network address, and is expressed as a decimal number. For example, all IPv6 addresses that start with the first byte of 73 (hexadecimal) could be expressed as 73:0:0:0:0:0:0:0/8 or 73::/8.

To generate an IPv6 global unicast address for the switch, complete the following steps:

1. From the global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. From the interface prompt, type “ipv6 address *ipv6-address*” or “ipv6 address *ipv6-address/prefix-length*,” where “prefix-length” indicates the address bits used to form the network portion of the address. (The network address starts from the left of the prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type “ipv6 default-gateway *gateway*,” where “gateway” is the IPv6 address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)#end
Console#show ipv6 interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-0C-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
IPv6 is enabled.
Link-local address:
  fe80::260:3eff:fe11:6700%1/64
```

```
Global unicast address(es):
  2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
ff02::1:ff00:0
ff02::1:ff11:6700
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#show ipv6 default-gateway
IPv6 default gateway 2001:db8:2222:7272::254
Console#
```

Dynamic Configuration

Obtaining an IPv4 Address

If you select the “bootp” or “dhcp” option, the system will immediately start broadcasting service requests. IP will be enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway. If the DHCP/BOOTP server is slow to respond, you may need to use the “ip dhcp restart client” command to re-start broadcasting service requests.

Note that the “ip dhcp restart client” command can also be used to start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. It may be necessary to use this command when DHCP is configured on a VLAN, and the member ports which were previously shut down are now enabled.

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
 - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
 - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
3. Type “end” to return to the Privileged Exec mode. Press <Enter>.

4. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.
5. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-0C-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.4 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): GEL-2861
  DHCP Relay Server:
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Obtaining an IPv6 Address

Link Local Address — There are several ways to configure IPv6 addresses. The simplest method is to automatically generate a “link local” address (identified by an address prefix in the range of FE80~FEBF). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

To generate an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ipv6 enable” and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  fe80::2e0:cff:fe00:fd%1/64
Global unicast address(es):
  2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
  ff02::1:ff00:0
  ff02::1:ff11:6700
  ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
```

```
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

```
Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to respond to SNMP requests or generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see [snmp-server view](#) command).

Community Strings (for SNMP version 1 and 2c clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- ◆ **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- ◆ **private** - with read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string

and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)

2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```



Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the “snmp-server host” command. From the Privileged Exec level global configuration mode prompt, type:

```
“snmp-server host host-address community-string [version {1 | 2c | 3 {auth |
noauth | priv}}]”
```

where “host-address” is the IP address for the trap receiver, “community-string” specifies access rights for a version 1/2c host, or is the user name of a version 3 host, “version” indicates the SNMP client version, and “auth | noauth | priv” means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see the [snmp-server host](#) command. The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called “mib-2” that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call “r&d” and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth read mib-2 write 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
des56 einstien
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to [“SNMP Commands” on page 159](#) or to the *Web Management Guide*.

Managing System Files

The switch’s flash memory supports three types of system files that can be managed by the CLI program, the web interface, or SNMP. The switch’s file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The types of files are:

- ◆ **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via FTP/SFTP/TFTP to a server for backup. The file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the switch will also create a file named “startup1.cfg” that contains system settings for switch initialization, including information about the unit identifier, and MAC address for the switch. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See [“Saving or Restoring Configuration Settings” on page 53](#) for more information.
- ◆ **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces.
- ◆ **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).



Note: The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/SFTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 32 Mbytes of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Upgrading the Operation Code

The following example shows how to download new firmware to the switch and activate it. The TFTP server could be any standards-compliant server running on Windows or Linux. When downloading from an FTP server, the logon interface will prompt for a user name and password configured on the remote server. Note that “anonymous” is set as the default user name.

File names on the switch are case-sensitive. The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, “,” “-”)

```

Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
1. config: 2. opcode: 2
Source file name: level1-xx61_V1.2.2.9.bix
Destination file name: level1-xx61_V1.2.2.9.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode: level1-xx61_V1.2.2.9.bix
Console(config)#exit
Console#dir
File Name                               Type      Startup Modified Time          Size (bytes)
-----
Unit 1:
level1-xx61_V1.2.2.9.bix                OpCode    Y          2018-03-21 09:22:07        8,798,472
Factory_Default_Config.cfg              Config    N          2016-04-13 05:28:36          477
startup1.cfg                            Config    Y          2017-08-15 08:14:31         1,381
-----
Free space for compressed user config files: 15,007,744
Total space: 33,554,432
Console#

```

Saving or Restoring Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes

(\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, ",", "-", "_")

There can be more than one user-defined configuration file saved in the switch's flash memory, but only one is designated as the "startup" file that is loaded when the switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config:<filename>** command.

The maximum number of saved configuration files depends on available flash memory. The amount of available flash memory can be checked by using the **dir** command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

To restore configuration settings from a backup server, enter the following command:

1. From the Privileged Exec mode prompt, type "copy tftp startup-config" and press <Enter>.
2. Enter the address of the TFTP server. Press <Enter>.
3. Enter the name of the startup file stored on the server. Press <Enter>.
4. Enter the name for the startup file on the switch. Press <Enter>.

```
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:

Success.
Console#
```

Automatic Installation of Operation Code and Configuration Settings

Downloading Operation Code from a File Server

Automatic Operation Code Upgrade can automatically download an operation code file when a file newer than the currently installed one is discovered on the file server. After the file is transferred from the server and successfully written to the file system, it is automatically set as the startup file, and the switch is rebooted.

Usage Guidelines

- ◆ If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- ◆ FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- ◆ The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- ◆ The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the "/" to indicate this (e.g., ftp://192.168.0.1/).
- ◆ The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be level1-xx61.bix (using lower case letters as indicated).
- ◆ The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.
- ◆ The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept *level1-xx61.BIX* from the server even though *level1-xx61.bix* was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unix-like systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are case-sensitive, meaning that two files in the same directory, *level1-xx61.bix* and *Level1-xx61.BIX* are considered to be unique files. Thus, if the upgrade file is stored as *Level1-xx61.BIX* (or even *LEVEL1-xx61.bix*) on a case-sensitive server, then the switch (requesting *Level1-xx61.BIX*) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

- ◆ Note that the switch itself does not distinguish between upper and lower-case file names, and only checks to see if the file stored on the server is more recent than the current runtime image.
- ◆ If two operation code image files are already stored on the switch's file system, then the non-startup image is deleted before the upgrade image is transferred.
- ◆ The automatic upgrade process will take place in the background without impeding normal operations (data switching, etc.) of the switch.
- ◆ During the automatic search and transfer process, the administrator cannot transfer or update another operation code image, configuration file, public key, or HTTPS certificate (i.e., no other concurrent file management operations are possible).
- ◆ The upgrade operation code image is set as the startup image after it has been successfully written to the file system.
- ◆ The switch will send an SNMP trap and make a log entry upon all upgrade successes and failures.
- ◆ The switch will immediately restart after the upgrade file is successfully written to the file system and set as the startup image.

To enable automatic upgrade, enter the following commands:

1. Specify the TFTP or FTP server to check for new operation code.

- When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
tftp://192.168.0.1[/filedir]/
```

- When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
ftp://[username[:password@]]192.168.0.1[/filedir]/
```

If the user name is omitted, "anonymous" will be used for the connection. If the password is omitted a null string ("") will be used for the connection.

If no user name nor password is required for the connection, then the "@" character cannot be used in the path name.

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/  
Console(config)#
```


This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://site9:billy@192.168.0.1/sm24/  
Console(config)#
```

2. Set the switch to automatically reboot and load the new code after the opcode upgrade is completed.

```
Console(config)#upgrade opcode reload  
Console(config)#
```

3. Set the switch to automatically upgrade the current operational code when a new version is detected on the server. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:
 - a. It will search for a new version of the image at the location specified by **upgrade opcode path** command. The name for the new image stored on the FTP/SFTP/TFTP server must be *level1-xx61.bix*. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.
 - b. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.
 - c. It sets the new version as the startup image.
 - d. It then restarts the system to start using the new image.

```
Console(config)#upgrade opcode auto  
Console(config)#
```

4. Display the automatic upgrade settings.

```
Console#show upgrade  
Auto Image Upgrade Global Settings:  
  Status      : Enabled  
  Reload Status : Enabled  
  Path        :  
  File Name   : level1-xx61_V1.2.2.1.bix  
Console#
```

The following shows an example of the upgrade process.

```

Console#dir
File Name                               Type   Startup Modified Time      Size (bytes)
-----
Unit 1:
level1-xx61_V1.2.2.1.bix                OpCode N      2017-10-27 10:05:27    9,130,248
level1-xx61_V1.2.2.3.bix                OpCode Y      2018-03-21 09:22:07    8,798,472
Factory_Default_Config.cfg              Config N      2016-04-13 05:28:36      477
startup1.cfg                            Config Y      2017-08-15 08:14:31     1,381
-----
Free space for compressed user config files: 24,137,992
Total space: 33,554,432

Press ENTER to start session
Automatic Upgrade is looking for a new image
New image detected: current version V1.2.2.3; new version V1.2.2.9
Image upgrade in progress
Downloading new image
Flash programming started
Flash programming completed
Success
The switch will now restart
...
Press ENTER to start session
Automatic Upgrade is looking for a new image
No new image detected
User Access Verification

Username: admin
Password:

CLI session with the GEL-2861 is opened.
To end the CLI session, enter [Exit].

Console#dir
File Name                               Type   Startup Modified Time      Size (bytes)
-----
Unit 1:
level1-xx61_V1.2.2.3.bix                OpCode N      2017-10-27 10:05:27    9,130,248
level1-xx61_V1.2.2.9.bix                OpCode Y      2018-03-21 09:22:07    8,798,472
Factory_Default_Config.cfg              Config N      2016-04-13 05:28:36      477
startup1.cfg                            Config Y      2017-08-15 08:14:31     1,381
-----
Free space for compressed user config files: 15,007,744
Total space: 33,554,43

Console#

```

Specifying a DHCP Client Identifier

DHCP servers index their database of address bindings using the client's Media Access Control (MAC) Address or a unique client identifier. The client identifier is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.

DHCP client Identifier (Option 60) is used by DHCP clients to specify their unique identifier. The client identifier is optional and can be specified while configuring DHCP on the primary network interface. DHCP Option 60 is disabled by default.

The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60 (vendor-class-identifier), 66 (tftp-server-name) and 67 (bootfile-name) statements can be added to the server daemon's configuration file as described in the following section.

If the DHCP server has an index entry for a switch requesting service, it should reply with the TFTP server name and boot file name. Note that the vendor class identifier can be formatted in either text or hexadecimal, but the format used by both the client and server must be the same.

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

Downloading a Configuration File and Other Parameters from a DHCP Server

Information passed on to the switch from a DHCP server may also include a configuration file to be downloaded and the TFTP servers where that file can be accessed, as well as other parameters. If the Factory Default Configuration file is used to provision the switch at startup, in addition to requesting IP configuration settings from the DHCP server, it will also ask for the name of a bootup configuration file and TFTP servers where that file is stored.

If the switch receives information that allows it to download the remote bootup file, it will save this file to a local buffer, and then restart the provision process.

Note the following DHCP client behavior:

- ◆ To enable dynamic provisioning via a DHCP server, this feature must be enabled using the `ip dhcp dynamic-provision` command.
- ◆ The bootup configuration file received from a TFTP server is stored on the switch with the original file name. If this file name already exists in the switch, the file is overwritten.
- ◆ If the name of the bootup configuration file is the same as the Factory Default Configuration file, the download procedure will be terminated, and the switch will not send any further DHCP client requests.
- ◆ If the switch fails to download the bootup configuration file based on information passed by the DHCP server, it will not send any further DHCP client requests.
- ◆ If the switch does not receive a DHCP response prior to completing the bootup process, it will continue to send a DHCP client request once a minute. These

requests will only be terminated if the switch's address is manually configured, but will resume if the address mode is set back to DHCP.

To successfully transmit a bootup configuration file to the switch, the DHCP daemon (using a Linux based system for this example) must be configured with the following information:

- ◆ Options 60, 66 and 67 statements can be added to the daemon's configuration file.

Table 1: Options 60, 66 and 67 Statements

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

- ◆ By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides these items, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 2: Options 55 and 124 Statements

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

The following configuration example is provided for a Linux-based DHCP daemon (dhcpd.conf file). In the "Vendor class" section, the server will always send Option 66 and 67 to tell the switch to download the "test" configuration file from server 192.168.255.101.

```
ddns-update-style ad-hoc;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

server-name "Server1";
Server-identifier 192.168.255.250;
#option 66, 67
option space dynamicProvision code width 1 length 1 hash size 2;
option dynamicProvision.tftp-server-name code 66 = text;
```

```
option dynamicProvision.bootfile-name code 67 = text;

subnet 192.168.255.0 netmask 255.255.255.0 {
    range 192.168.255.160 192.168.255.200;
    option routers 192.168.255.101;
    option tftp-server-name "192.168.255.100"; #Default Option 66
    option bootfile-name "bootfile";          #Default Option 67
}

class "Option66,67_1" {                      #DHCP Option 60 Vendor class
two
    match if option vendor-class-identifier = "gel-1061";
    option tftp-server-name "192.168.255.101";
    option bootfile-name "test";
}
```



Note: Use "gel-1061" for the vendor-class-identifier in the dhcpd.conf file.

Setting the System Clock

Simple Network Time Protocol (SNTP) or Network Time Protocol (NTP) can be used to set the switch's internal clock based on periodic updates from a time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP or NTP, the switch will only record the time from the factory default set at the last bootstrap.



Caution: It is strongly advised to use SNTP or NTP to maintain an accurate record of switch events. Manually setting the system clock can result in an inaccurate time-stamp on system events.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

The switch also supports the following time settings:

- ◆ Time Zone – You can specify the offset from Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).
- ◆ Summer Time/Daylight Saving Time (DST) – In some regions, the time shifts by one hour in the fall and spring. The switch supports manual entry for one-time or recurring clock shifts.

Setting the Time Manually

To manually set the clock to 10:30:36, July 29th, 2018, enter this command.

```
Console#calendar set 10 30 36 29 July 2018
Console#
```

To set the time zone, enter a command similar to the following.

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

To set the time shift for summer time, enter a command similar to the following.

```
Console(config)#clock summer-time SUMMER date 2 april 2013 0 0 30 june 2013 0
0
Console(config)#
```

To display the clock configuration settings, enter the following command.

```
Console#show calendar
Current Time      : Jul 28 00:54:20 2015
Time Zone        : Japan, 08:00
Summer Time      : SUMMER, offset 60 minutes
                  Apr 2 2013 00:00 to Jun 30 2015 00:00
Summer Time in Effect : Yes
Console#
```

Configuring SNTP

Setting the clock based on an SNTP server can provide more accurate clock synchronization across network switches than manually-configured time. To configure SNTP, set the switch as an SNTP client, and then set the polling interval, and specify a time server as shown in the following example.

```
Console(config)#sntp client
Console(config)#sntp poll 60
Console(config)#sntp server 10.1.0.19
Console(config)#exit
Console#show sntp
Current Time      : Apr 2 16:06:07 2013
Poll Interval     : 60 seconds
Current Mode      : Unicast
SNTP Status       : Enabled
SNTP Server       : 10.1.0.19
Current Server    : 10.1.0.19
Console#
```

Configuring NTP Requesting the time from an NTP server is the most secure method. You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

When more than one time server is configured, the client will poll all of the time servers, and compare the responses to determine the most reliable and accurate time update for the switch.

To configure NTP time synchronization, enter commands similar to the following.

```

Console(config)#ntp client
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#ntp authenticate
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#exit
Console#show ntp
Current Time           : Apr 29 13:57:32 2011
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server  : 192.168.0.88      Port: 123
Last Update Time        : Mar 12 02:41:01 2013 UTC
NTP Server 192.168.0.88 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885

Current Time           : Apr  2 16:28:34 2013
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server  : 192.168.5.23      Port: 0
Last Update Time        : Apr  2 16:00:00 2013 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.5.23 version 3 key 19
NTP Authentication Key 45 md5 2662T75S5658RU5424180034777
Console#

```


Section II

Command Line Interface

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

- ◆ [“Using the Command Line Interface” on page 67](#)
- ◆ [“General Commands” on page 79](#)
- ◆ [“System Management Commands” on page 87](#)
- ◆ [“SNMP Commands” on page 159](#)
- ◆ [“Remote Monitoring Commands” on page 185](#)
- ◆ [“Flow Sampling Commands” on page 193](#)
- ◆ [“Authentication Commands” on page 199](#)
- ◆ [“General Security Measures” on page 259](#)
- ◆ [“Access Control Lists” on page 325](#)
- ◆ [“Interface Commands” on page 349](#)
- ◆ [“Link Aggregation Commands” on page 379](#)
- ◆ [“Power over Ethernet Commands” on page 393](#)
- ◆ [“Port Mirroring Commands” on page 403](#)
- ◆ [“Congestion Control Commands” on page 413](#)
- ◆ [“Loopback Detection Commands” on page 419](#)
- ◆ [“Address Table Commands” on page 425](#)

- ◆ “Spanning Tree Commands” on page 431
- ◆ “VLAN Commands” on page 461
- ◆ “Class of Service Commands” on page 489
- ◆ “Quality of Service Commands” on page 501
- ◆ “Multicast Filtering Commands” on page 513
- ◆ “LLDP Commands” on page 573
- ◆ “Domain Name Service Commands” on page 597
- ◆ “DHCP Commands” on page 599
- ◆ “IP Interface Commands” on page 621
- ◆ “IP Routing Commands” on page 659

2

Using the Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).



Note: You can only access the console interface through the Master unit in the stack.

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:
  CLI session with the GEL-2861 is opened.
  To end the CLI session, enter [Exit].

Console#
```

Telnet Connection Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).



Note: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address or host name of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-*n*” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-*n*>” for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

CLI session with the GEL-2861 is opened.
To end the CLI session, enter [Exit].

Vty-0#
```



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

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- ◆ To enter a simple command, enter the command keyword.
- ◆ To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter the following commands. The default password “super” is used to change from Normal Exec to Privileged Exec mode:

```
Console>enable
Password:
Console#show startup-config
```

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

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Console#show ?
  access-group      Access groups
  access-list       Access lists
  accounting         Uses the specified accounting list
  arp               Information of ARP cache
  authorization      Enables EXEC accounting
  bridge-ext        Bridge extension information
  cable-diagnostics Shows the information of cable diagnostics
  calendar           Date and time information
  class-map          Displays class maps
  cluster            Display cluster
  debug             State of each debugging option
  dns               DNS information
  dos-protection     Shows the system dos-protection summary information
  dot1q-tunnel       802.1Q tunnel
  dot1x             802.1X content
  history            Shows history information
  hosts             Host information
  interfaces         Shows interface information
  ip                IP information
  ipv6              IPv6 information
  lacp              LACP statistics
  line              TTY line information
  lldp              LLDP
  log               Log records
  logging            Logging setting
  loopback-detection Shows loopback detection information
  mac               MAC access list
  mac-address-table Configuration of the address table
  mac-vlan          MAC-based VLAN information
  management        Shows management information
  memory            Memory utilization
  network-access     Shows the entries of the secure port.
  nlm               Show notification log
  ntp               Network Time Protocol configuration
  policy-map         Displays policy maps
  port              Port characteristics
  port-channel       Port channel information
  power             Shows power
  power-save         Shows the power saving information
  privilege          Shows current privilege level
  process           Device process
  protocol-vlan      Protocol-VLAN information
  public-key         Public key information
  qos               Quality of Service
  queue             Priority queue information
  radius-server      RADIUS server information
  reload            Shows the reload settings
  rmon              Remote monitoring information
  rspan             Display status of the current RSPAN configuration
```

```
running-config    Information on the running configuration
sflow             Shows the sflow information
snmp              Simple Network Management Protocol configuration and
                  statistics
snmp-server       Displays SNMP server configuration
snmp              Simple Network Time Protocol configuration
spanning-tree     Spanning-tree configuration
ssh              Secure shell server connections
startup-config    Startup system configuration
system            System information
tacacs-server     TACACS server information
tech-support      Technical information
time-range        Time range
traffic-segmentation Traffic segmentation information
upgrade           Shows upgrade information
users             Information about users logged in
version           System hardware and software versions
vlan              Shows virtual LAN settings
voice             Shows the voice VLAN information
watchdog          Displays watchdog status
web-auth          Shows web authentication configuration
Console#
```

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

```
Console#show interfaces ?
brief             Shows brief interface description
counters          Interface counters information
history           Historical sample of interface counters information
protocol-vlan     Protocol-VLAN information
status            Shows interface status
switchport        Shows interface switchport information
transceiver       Interface of transceiver information
transceiver-threshold Interface of transceiver-threshold information
Console#
```

Show commands which display more than one page of information (e.g., **show running-config**) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.

Partial Keyword Lookup If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Console#show s?
sflow          snmp          snmp-server    snmp          spanning-tree
ssh            startup-config system
Console#show s
```

Negating the Effect of Commands For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “?” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 3: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map DHCP IGMP Profile Interface Line Multiple Spanning Tree Policy Map Time Range VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.
You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The

system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password “super.”

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

CLI session with the GEL-2861 is opened.
To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

CLI session with the GEL-2861 is opened.
To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- ◆ Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- ◆ Access Control List Configuration - These commands are used for packet filtering.
- ◆ Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- ◆ IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- ◆ Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- ◆ Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.

- ◆ Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- ◆ Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- ◆ Time Range - Sets a time range for use by other functions, such as Access Control Lists.
- ◆ VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

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

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 4: Configuration Command Modes

Mode	Command	Prompt	Page
Access Control List	access-list arp	Console(config-arp-acl)	344
	access-list ip standard	Console(config-std-acl)	326
	access-list ip extended	Console(config-ext-acl)	326
	access-list ipv6 standard	Console(config-std-ipv6-acl)	332
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	332
	access-list mac	Console(config-mac-acl)	339
Class Map	class-map	Console(config-cmap)	502
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)	350
Line	line {console vty}	Console(config-line)	115
MSTP	spanning-tree mst-configuration	Console(config-mstp)	437
Policy Map	policy-map	Console(config-pmap)	505
Time Range	time-range	Console(config-time-range)	149
VLAN	vlan database	Console(config-vlan)	462

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
Console(config-if)#exit
Console(config)#
```

Command Line Processing Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 5: Keystroke Commands

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

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

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

```

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

```

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

CLI Command Groups

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

Table 6: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	79
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, and the system clock	87
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	159
Remote Monitoring	Supports statistics, history, alarm and event groups	185
User Authentication	Configures user names and passwords, command privilege levels, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses	199
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	259
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header), or non-IP frames (based on MAC address or Ethernet type)	325
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	349
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	379
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	403
Congestion Control	Sets the input/output rate limits, traffic storm thresholds, and thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.	413
Loopback Detection	Detects general loopback conditions caused by hardware problems or faulty protocol settings	419

Table 6: Command Group Index (Continued)

Command Group	Description	Page
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	425
Spanning Tree	Configures Spanning Tree settings for the switch	431
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	461
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for DSCP	489
Quality of Service	Configures Differentiated Services	501
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration, and IPv6 MLD snooping	513
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	573
Domain Name Service	Configures DNS services.	597
Dynamic Host Configuration Protocol	Configures DHCP client and relay functions	599
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters	621
IP Routing	Configures static and dynamic unicast routing	659
Debug	Displays debugging information for all key functions	
	These commands are not described in this manual. Please refer to the prompt messages included in the CLI interface.	

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

ACL (Access Control List Configuration)
CM (Class Map Configuration)
GC (Global Configuration)
IC (Interface Configuration)
IPC (IGMP Profile Configuration)
LC (Line Configuration)
MST (Multiple Spanning Tree)
NE (Normal Exec)
PE (Privileged Exec)
PM (Policy Map Configuration)
VC (VLAN Database Configuration)

3

General Commands

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

Table 7: General Commands

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

prompt This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt.
(Maximum length: 32 characters)

Default Setting

Console

Command Mode

Global Configuration

Command Usage

This command and the [hostname](#) command can be used to set the command line prompt as shown in the example below. Using the **no** form of either command will restore the default command line prompt.

Example

```

Console(config)#prompt RD2
RD2(config)#

```

reload (Global Configuration) This command restarts the system at a specified time, after a specified delay, or at a periodic interval. You can reboot the system immediately, or you can configure the switch to reset after a specified amount of time. Use the **cancel** option to remove a configured setting.

Syntax

```

reload {at hour minute [{month day | day month} [year]] |
in {hour hours | minute minutes | hour hours minute minutes} |
regularly hour minute [period {daily | weekly day-of-week |
monthly day-of-month}] | cancel [at | in | regularly]}

```

reload at - A specified time at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

month - The month at which to reload. (january ... december)

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

year - The year at which to reload. (Range: 1970-2037)

reload in - An interval after which to reload the switch.

hours - The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)

minutes - The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)

reload regularly - A periodic interval at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

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

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

reload cancel - Cancels the specified reload option.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ This command resets the entire system.
- ◆ Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.
- ◆ When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the [copy running-config startup-config](#) command (See [“copy” on page 103](#)).

Example

This example shows how to reset the switch after 30 minutes:

```

Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 2016 ---
***

Are you sure to reboot the system at the specified time? <y/n>

```

enable This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See [“Understanding Command Modes” on page 72](#).

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec,
15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- ◆ “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the [enable password](#) command.)

- ◆ The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

[disable \(84\)](#)

[enable password \(200\)](#)

quit This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

show history This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```

Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#

```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```

Console#!2
Console#config
Console(config)#

```

configure This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration. See [“Understanding Command Modes” on page 72](#).

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#configure
Console(config)#

```

Related Commands

[end \(85\)](#)

disable This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See [“Understanding Command Modes” on page 72](#).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

[enable \(81\)](#)

reload (Privileged Exec) This command restarts the system.



Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

show reload This command displays the current reload settings, and the time at which next scheduled reload will take place.

Command Mode

Privileged Exec

Example

```
Console#show reload
Reloading switch in time:                0 hours 29 minutes.

The switch will be rebooted at January  1 02:11:50 2015.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

end This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

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

Press ENTER to start session

User Access Verification

Username:
```

4

System Management Commands

The system management commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 8: System Management Commands

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
System Status	Displays system configuration, active managers, and version information
Frame Size	Enables support for jumbo frames
File Management	Manages code image or switch configuration files
Line	Sets communication parameters for the serial port, including baud rate and console time-out
Event Logging	Controls logging of error messages
SMTP Alerts	Configures SMTP email alerts
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually
Time Range	Sets a time range for use by other functions, such as Access Control Lists
Switch Clustering	Configures management of multiple devices via a single IP address

Device Designation

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

Table 9: Device Designation Commands

Command	Function	Mode
hostname	Specifies the host name for the switch	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC

hostname This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*

no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The host name specified by this command is displayed by the [show system](#) command and on the Show > System web page.
- ◆ This command and the [prompt](#) command can be used to set the command line prompt as shown in the example below. Using the **no** form of either command will restore the default command line prompt.

Example

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

System Status

This section describes commands used to display system information.

Table 10: System Status Commands

Command	Function	Mode
show access-list tcam-utilization	Shows utilization parameters for TCAM	PE
show memory	Shows memory utilization parameters	PE
show process cpu	Shows CPU utilization parameters	PE
show process cpu guard	Shows the CPU utilization watermark and threshold	NE
show process cpu task	Shows CPU utilization per process	NE, PE
show running-config	Displays the configuration data currently in use	PE
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show system	Displays system information	NE, PE

Table 10: System Status Commands (Continued)

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

show access-list This command shows utilization parameters for TCAM (Ternary Content
tcam-utilization Addressable Memory), including the number policy control entries in use, and the number of free entries.

Command Mode
Privileged Exec

Command Usage

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

Example

```
Console#show access-list tcam-utilization
Pool capability code:
AM - MAC ACL, A4 - IPv4 ACL, A6S - IPv6 Standard ACL,
A6E - IPv6 extended ACL, DM - MAC diffServ, D4 - IPv4 diffServ,
D6S - IPv6 standard diffServ, D6E - IPv6 extended diffServ,
W - Web authentication, I - IP source guard, C - CPU interface,
L - Link local, MV - Mac based VLAN, PV - Protocol based VLAN,
VV - Voice VLAN, R - Routing, Reserved - Reserved,
ALL - All supported function,
```

Unit	Device	Pool	Total	Used	Free	Capability
1	0	0	128	128	0	R
1	0	1	64	0	64	A6S A6E
1	0	2	128	0	128	A4
1	0	3	128	0	128	AM
1	0	4	64	0	64	D6S D6E
1	0	5	128	0	128	D4 W
1	0	6	128	0	128	DM
1	0	7	128	1	127	MV PV VV
1	0	8	64	0	64	I
1	0	9	64	64	0	C

```
1      0   10   64   64   0 Reserved
1      0   11   64   64   0 C L
```

Console#

Table 11: show access-list tcam-utilization - display description

Field	Description
Pool Capability Code	Abbreviation for processes shown in the TCAM List.
Unit	Stack unit identifier.
Device	Memory chip used for indicated pools.
Pool	Rule slice (or call group). Each slice has a fixed number of rules that are used for the specified features.
Total	The maximum number of policy control entries allocated to the each pool.
Used	The number of policy control entries used by the operating system.
Free	The number of policy control entries available for use.
Capability	The processes assigned to each pool.

show memory This command shows memory utilization parameters, and alarm thresholds.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command shows the amount of memory currently free for use, the amount of memory allocated to active processes, the total amount of system memory, and the alarm thresholds.

Example

```
Console#show memory
Status Bytes      %
-----
Free    111706112  41
Used    156729344  59
Total   268435456

Alarm Configuration
Rising Threshold      : 95%
Falling Threshold     : 90%

Console#
```

Related Commands

[memory \(180\)](#)

show process cpu This command shows the CPU utilization parameters, alarm status, and alarm thresholds.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 24%

CPU Utilization in the past 60 seconds
Average Utilization      : 24%
Maximum Utilization      : 25%

Alarm Status
Current Alarm Status     : Off
Last Alarm Start Time    : Dec 31 00:00:19 2000
Last Alarm Duration Time : 15 seconds

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

Console#
```

Related Commands

[process cpu \(181\)](#)

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

Command Mode

Normal Exec, Privileged Exec

Example

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

Console#
```

Table 12: show process cpu guard - display description

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

Related Commands

[process cpu guard \(182\)](#)

show process cpu task This command shows the CPU utilization per process.

Command Mode

Normal Exec, Privileged Exec

Example

Console#show process cpu task			
Task	Util (%)	Avg (%)	Max (%)
-----	-----	-----	-----
APP_PROTOCOL_GR	0.00	0.00	0.00
APP_PROTOCOL_PR	0.00	0.00	0.00
CFGDB_TD	0.40	0.19	0.40
CLI_PROC	0.00	0.00	0.00
CLITASK0	0.00	0.00	0.00
DHCPSPNP_GROUP	0.00	0.00	0.00
DHCPSPNP_TD	0.00	0.00	0.00
DNS_PROXY_TD	0.00	0.00	0.00
DNS_RESOL_TD	0.00	0.00	0.00
DRIVER_GROUP	5.80	5.44	6.20
DRIVER_GROUP_TW	0.00	0.00	0.00
HTTP_TD	0.00	0.00	0.00
IP_SERVICE GROU	0.00	0.00	0.00
L2_L4_PROCESS	0.00	0.00	0.00
L2MCAST_GROUP	0.00	0.00	0.00
L2MUX_GROUP	0.00	0.00	0.00

L4_GROUP	0.00	0.00	0.00
LACP_GROUP	0.00	0.00	0.00
MDNS_GROUP	0.00	0.00	0.00
NETACCESS_GROUP	0.00	0.00	0.00
NETACCESS_HASH2	0.00	0.00	0.00
NETACCESS_NMTR	0.20	0.10	0.40
NIC	0.00	0.00	0.00
NMTRDRV	1.00	0.84	1.40
NSM_PROC	0.00	0.00	0.00
NSM_TD	0.00	0.00	0.00
RADIUS	0.00	0.00	0.00
RIP_GROUP	0.00	0.00	0.00
RIP_PROC	0.00	0.00	0.00
SFLOW_GROUP	0.00	0.00	0.00
SFLOW_PROC	0.00	0.00	0.00
SFLOW_TD	0.00	0.00	0.00
SNMP_GROUP	0.00	0.00	0.00
SNMP_TD	0.00	0.03	0.20
SSH_GROUP	0.00	0.00	0.00
STA_GROUP	0.00	0.00	0.00
STKCTRL_GROUP	0.00	0.00	0.00
STKTPLG_PROC	0.00	0.00	0.00
SWCTRL_GROUP	0.00	0.00	0.00
SWCTRL_TD	0.00	0.00	0.00
SWDRV_MONITOR	0.00	0.00	0.00
sys_debug_proc	0.00	0.00	0.00
SYSMGMT_GROUP	0.00	0.01	0.20
SYSTEM	2.20	1.84	2.40
UTILITY_GROUP	0.00	0.00	0.00
WEB_PROC	0.00	0.00	0.00
WTDog_PROC	0.00	0.00	0.00
XFER_TD	0.00	0.00	0.00
Console#			

show running-config This command displays the configuration information currently in use.

Syntax

show running-config [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **interface** keyword to display configuration data for the specified interface.

- ◆ Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- ◆ This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - MAC address for
 - SNMP community strings
 - Users (names, access levels, and encrypted passwords)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - Multiple spanning tree instances (name and interfaces)
 - IP address configured for VLANs
 - Spanning tree settings
 - Interface settings
 - Any configured settings for the console port and Telnet
- ◆ For security reasons, user passwords are only displayed in encrypted format.

Example

```
Console#show running-config
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_03</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
enable password 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
VLAN 1 name DefaultVlan media ethernet
!
spanning-tree mst configuration
!
interface ethernet 1/1
no negotiation
...
interface ethernet 1/28
no negotiation
!
interface vlan 1
ip address dhcp
!
interface vlan 1
!
line console
!
line vty
!
end
!
Console#
```

Related Commands

[show startup-config \(95\)](#)

show startup-config This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Command Mode

Privileged Exec

Command Usage

- ◆ Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- ◆ This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - MAC address for
 - SNMP community strings
 - SNMP trap authentication
 - Users (names and access levels)
 - VLAN database (VLAN ID, name and state)
 - Multiple spanning tree instances (name and interfaces)
 - Interface settings and VLAN configuration settings for each interface
 - IP address for VLANs
 - Any configured settings for the console port and Telnet

Example

Refer to the example for the running configuration file.

Related Commands

[show running-config \(93\)](#)

show system This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show system
System Description : GEL-2861
System OID String  : 1.3.6.1.4.1.22426.43.104
System Information
```

```
System Up Time      : 0 days, 1 hours, 25 minutes, and 46.64 seconds
System Name         :
System Location      :
System Contact       :
MAC Address (Unit 1) : A8-2B-B5-73-59-60
Web Server           : Enabled
Web Server Port      : 80
Web Secure Server    : Enabled
Web Secure Server Port : 443
Telnet Server        : Enabled
Telnet Server Port   : 23
Jumbo Frame          : Disabled
Unit 1

Main Power Status    : Up
Console#
```

Table 13: show system – display description

Parameter	Description
System Description	Brief description of device type.
System OID String	MIB II object ID for switch's network management subsystem.
System Up Time	Length of time the management agent has been up.
System Name	Name assigned to the switch system.
System Location	Specifies the system location.
System Contact	Administrator responsible for the system.
MAC Address	MAC address assigned to this switch.
Web Server/Port	Shows administrative status of web server and UDP port number.
Web Secure Server/Port	Shows administrative status of secure web server and UDP port number.
Telnet Server/Port	Shows administrative status of Telnet server and TCP port number.
Jumbo Frame	Shows if jumbo frames are enabled or disabled.
System Temperature	Temperature at specified thermal detection point.
Main Power Status	Displays the status of the internal power supply.
Redundant Power Status	Displays the status of the redundant power supply.

show tech-support This command displays a detailed list of system settings designed to help technical support resolve configuration or functional problems.

Command Mode
Privileged Exec

Command Usage

This command generates a long list of information including detailed system and interface settings. It is therefore advisable to direct the output to a file using any suitable output capture function provided with your terminal emulation program.

Example

```
User Access Verification

Username: admin
Password:

      CLI session with the GEL-2861 is opened.
      To end the CLI session, enter [Exit].

Console#show tech-support

dir:
File Name                                Type      Startup Modified Time      Size (bytes)
-----
Unit 1:
level1-xx61_V1.2.2.9.bix                 OpCode    Y          2018-03-21 09:22:07      8,798,472
Factory_Default_Config.cfg               Config    N          2016-04-13 05:28:36        477
startup1.cfg                             Config    Y          2017-08-15 08:14:31       1,381
-----
Free space for compressed user config files: 24,137,992
Total space: 33,554,43

show arp:
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address      Type      Interface
-----
192.168.2.99    F0-79-59-8F-2B-FE dynamic      VLAN 1

Total entry : 1

show interfaces brief:
Interface Name      Status      PVID Pri Speed/Duplex  Type      Trunk
-----
Eth 1/ 1            Up          1    0   Auto-100full  1000BASE-T  None
Eth 1/ 2            Down        1    0   Auto-100full  1000BASE-T  None
Eth 1/ 3            Down        1    0   Auto-100full  1000BASE-T  None
Eth 1/ 4            Down        1    0   Auto-100full  1000BASE-T  None
Eth 1/ 5            Down        1    0   Auto-100full  1000BASE-T  None
...
```

show users Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
User Name Accounts:
User Name          Privilege  Public-Key
-----
admin              15 None
guest              0 None

Online Users:
Line      Session ID User Name          Idle Time (h:m:s) Remote IP Addr
-----
*Console          0 admin              0:00:01

Web Online Users:
Line      User Name          Idle Time (h:m:s) Remote IP Addr
-----

Console#
```

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

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show version
Unit 1
Serial Number      : EC1647000491
Hardware Version   : R01
Number of Ports    : 28
Main Power Status  : Up
Role               : Master
Loader Version     : 0.2.1.1
Linux Kernel Version : 2.6.19
Operation Code Version : 1.2.2.9

Console#
```

Table 14: show version – display description

Parameter	Description
Serial Number	The serial number of the switch.
Hardware Version	Hardware version of the main board.
Number of Ports	Number of built-in ports.
Main Power Status	Displays the status of the internal power supply.
Role	Shows that this switch is operating as Master or Slave.
Loader Version	Version number of loader code.
Linux Kernel Version	Version number of Linux kernel.
Operation Code Version	Version number of runtime code.

show watchdog This command shows if watchdog debugging is enabled.

Command Mode

Privileged Exec

Example

```
Console#show watchdog
Software Watchdog Information
Status :      Enabled
AutoReload :  Enabled
Console#
```

watchdog software This command monitors key processes, and automatically reboots the system if any of these processes are not responding correctly.

Syntax

watchdog software {disable | enable}

Default Setting

Enabled

Command Mode

Privileged Exec

Example

```
Console#watchdog software disable
Console#
```

Frame Size

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

Table 15: Frame Size Commands

Command	Function	Mode
jumbo frame	Enables support for jumbo frames	GC

jumbo frame This command enables support for layer 2 jumbo frames for Gigabit and 10 Gigabit Ethernet ports. Use the **no** form to disable it.

Syntax

[no] jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This switch provides more efficient throughput for large sequential data transfers by supporting layer 2 jumbo frames on Gigabit and 10 Gigabit Ethernet ports or trunks up to 10240 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- ◆ To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- ◆ The current setting for jumbo frames can be displayed with the [show system](#) command.

Example

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

Related Commands

[show system \(95\)](#)

[show ipv6 mtu \(645\)](#)

File Management

Managing Firmware

Firmware can be uploaded and downloaded to or from an FTP/SFTP/TFTP server. By saving runtime code to a file on an FTP/SFTP/TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from an FTP/SFTP/TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the FTP/SFTP/TFTP server, but cannot be used as the destination on the switch.

Table 16: Flash/File Commands

Command	Function	Mode
<i>General Commands</i>		
<code>boot system</code>	Specifies the file or image used to start up the system	GC
<code>copy</code>	Copies a code image or a switch configuration to or from flash memory or an FTP/SFTP/TFTP server	PE
<code>delete</code>	Deletes a file or code image	PE
<code>dir</code>	Displays a list of files in flash memory	PE
<code>whichboot</code>	Displays the files booted	PE
<i>Automatic Code Upgrade Commands</i>		
<code>upgrade opcode auto</code>	Automatically upgrades the current image when a new version is detected on the indicated server	GC
<code>upgrade opcode path</code>	Specifies an FTP/SFTP/TFTP server and directory in which the new opcode is stored	GC
<code>upgrade opcode reload</code>	Reloads the switch automatically after the opcode upgrade is completed	GC
<code>show upgrade</code>	Shows the opcode upgrade configuration settings.	PE
<i>TFTP Configuration Commands</i>		
<code>ip tftp retry</code>	Specifies the number of times the switch can retry transmitting a request to a TFTP server	GC
<code>ip tftp timeout</code>	Specifies the time the switch can wait for a response from a TFTP server before retransmitting a request or timing out for the last retry	GC
<code>show ip tftp</code>	Displays information about TFTP settings	PE

General Commands

boot system This command specifies the file or image used to start up the system.

Syntax

boot system [*unit no.:*] {**config** | **opcode** {: *filename*}}

config* - Configuration file.

opcode* - Run-time operation code.

unit no. - Unit number of the switch (followed by a colon(:))

filename - Name of configuration file or code image.

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ A colon (:) is required after the specified file type.
- ◆ If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system :1 config: startup
Console(config)#
```

Related Commands

[dir \(108\)](#)

[whichboot \(109\)](#)

copy This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/SFTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/SFTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/SFTP/TFTP server and the quality of the network connection.

Syntax

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

copy ftp {add-to-running-config | file | https-certificate | public-key | running-config | sftp | startup-config}

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

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

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

add-to-running-config - Keyword that adds the settings listed in the specified file to the running configuration.

file - Keyword that allows you to copy to/from a file.

ftp - Keyword that allows you to copy to/from an FTP server.

https-certificate - Keyword that allows you to copy the HTTPS secure site certificate.

public-key - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell" on page 234.)

running-config - Keyword that allows you to copy to/from the current running configuration.

sftp - Keyword that copies a file to or from an SFTP server.

startup-config - The configuration used for system initialization.

tftp - Keyword that allows you to copy to/from a TFTP server.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ The system prompts for data required to complete the copy command.
- ◆ The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 127 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

- ◆ The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.
- ◆ You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- ◆ To replace the startup configuration, you must use **startup-config** as the destination.
- ◆ The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/SFTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- ◆ For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" in the *Web Management Guide*. For information on configuring the switch to use HTTPS for a secure connection, see the [ip http secure-server](#) command.
- ◆ The reload command will not be accepted during copy operations to flash memory.
- ◆ When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that "anonymous" is set as the default user name.
- ◆ When logging into a remote SFTP server, the interface prompts for a user name and password configured on the remote server. If this is a first time connection, the system checks to see if the public key offered by the server matches one stored locally. If not, the server's public key will be copied to the local system.
- ◆ Secure Shell FTP (SFTP) provides a method of transferring files between two network devices over an SSH2-secured connection. SFTP functions similar to Secure Copy (SCP), using SSH for user authentication and data encryption.

Although the underlying premises of SFTP are similar to SCP, it requires some additional steps to verify the protocol versions and perform security checks. SFTP connection setup includes verification of the DSS signature, creation of session keys, creation of client-server and server-client ciphers, SSH key exchange, and user authentication. An SFTP channel is then opened, the SFTP protocol version compatibility verified, and SFTP finally initialized.
- ◆ The reload command will not be accepted during copy operations to flash memory.

Example

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
  1. config:  2. opcode: 2
Source file name: m360.bix
```



```
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
  1. config:  2. opcode: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

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

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

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: *****
```

```
Success.  
Console#reload  
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key  
TFTP server IP address: 192.168.1.19  
Choose public key type:  
  1. RSA:  2. DSA: <1-2>: 1  
Source file name: steve.pub  
Username: steve  
TFTP Download  
Success.  
Write to FLASH Programming.  
Success.  
  
Console#
```

This example shows how to copy a file to an FTP server.

```
Console#copy ftp file  
FTP server IP address: 169.254.1.11  
User[anonymous]: admin  
Password[]: *****  
Choose file type:  
  1. config:  2. opcode: 2  
Source file name: BLANC.BIX  
Destination file name: BLANC.BIX  
Console#
```

This example shows how to copy a file from an SFTP server. Note that the public key offered by the server is not found on the local system, but is saved locally after the user selects to continue the copy operation.

```
Console#copy sftp file  
SFTP server IP address: 192.168.0.110  
Choose file type:  
  1. config:  2. opcode: 1  
Source file name: startup2.cfg  
Destination file name: startup2.cfg  
Login User Name: admin  
Login User Password:  
Press 'y' to allow connect to new sftp server,  
and 'N' to deny connect to new sftp server: y  
Success.  
Console#
```

delete This command deletes a file or image.

Syntax

delete {**file** {**unit** *unit no.* {**name** *filename*} | **name** *filename*} | **https-certificate** | **public-key** *username* [**dsa** | **rsa**]}

file - Keyword that allows you to delete a file.

name - Keyword indicating a name of a file.

filename - Name of configuration file or code image.

unit no. - Unit number of the switch

https-certificate - Keyword that allows you to delete the HTTPS secure site certificate. You must reboot the switch to load the default certificate.

public-key - Keyword that allows you to delete a SSH key on the switch.
(See [“Secure Shell” on page 234.](#))

username - Name of an SSH user. (Range: 1-32 characters)

dsa - DSA public key type.

rsa - RSA public key type.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ If the file type is used for system startup, then this file cannot be deleted.
- ◆ “Factory_Default_Config.cfg” cannot be deleted.
- ◆ If the public key type is not specified, then both DSA and RSA keys will be deleted.

Example

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

```
Console#delete file name test2.cfg
Console#
```

Related Commands

[dir \(108\)](#)

[delete public-key \(239\)](#)

dir This command displays a list of files in flash memory.

Syntax

dir {config | opcode}: [filename]}

config - Switch configuration file.

opcode - Run-time operation code image file.

filename - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

If you enter the command **dir** without any parameters, the system displays all files.

File information is shown below:

Table 17: File Directory Information

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

Example

The following example shows how to display all file information:

```
Console#dir
File Name                               Type   Startup Modified Time      Size (bytes)
-----
Unit 1:
level1-xx61_V1.2.2.9.bix                OpCode  Y      2018-03-21 09:22:07  8,798,472
Factory_Default_Config.cfg              Config  N      2016-04-13 05:28:36    477
startup1.cfg                            Config  Y      2017-08-15 08:14:31    1,381
-----
Free space for compressed user config files: 24,137,992
Total space: 33,554,43
Console#
```

whichboot This command displays which files were booted when the system powered up.

Syntax

whichboot

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

Console#whichboot				
File Name	Type	Startup	Modified Time	Size (bytes)

Unit 1:				
level1-xx61_V1.2.2.9.bix	OpCode	Y	2017-09-22 08:33:39	8,790,276
startup1.cfg	Config	Y	2017-09-22 08:31:08	1,380
Console#				

Automatic Code Upgrade Commands

upgrade opcode auto This command automatically upgrades the current operational code when a new version is detected on the server indicated by the [upgrade opcode path](#) command. Use the **no** form of this command to restore the default setting.

Syntax

[no] upgrade opcode auto

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This command is used to enable or disable automatic upgrade of the operational code. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:
 1. It will search for a new version of the image at the location specified by [upgrade opcode path](#) command. The name for the new image stored on the TFTP server must be level1-xx61.bix. If the switch detects a code version

newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.

2. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.
 3. It sets the new version as the startup image.
 4. It then restarts the system to start using the new image.
- ◆ Any changes made to the default setting can be displayed with the [show running-config](#) or [show startup-config](#) commands.

Example

```
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

If a new image is found at the specified location, the following type of messages will be displayed during bootstrap.

```
:
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
:
```

upgrade opcode path This command specifies an TFTP server and directory in which the new opcode is stored. Use the **no** form of this command to clear the current setting.

Syntax

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - The location of the new code.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ This command is used in conjunction with the `upgrade opcode auto` command to facilitate automatic upgrade of new operational code stored at the location indicated by this command.
- ◆ The name for the new image stored on the TFTP server must be level1-xx61_V1.2.2.1.bix. However, note that file name is not to be included in this command.
- ◆ When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
tftp://192.168.0.1[/filedir]/
```

- ◆ When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
ftp://[username[:password@]]192.168.0.1[/filedir]/
```

If the user name is omitted, "anonymous" will be used for the connection. If the password is omitted a null string ("") will be used for the connection.

Example

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/  
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/  
Console(config)#
```

upgrade opcode reload This command reloads the switch automatically after the opcode upgrade is completed. Use the **no** form to disable this feature.

Syntax

[no] upgrade opcode reload

Default Setting

Disabled

Command Mode

Global Configuration

Example

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode reload
Console(config)#
```

show upgrade This command shows the opcode upgrade configuration settings.

Command Mode

Privileged Exec

Example

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status      : Disabled
  Reload Status : Disabled
  Path        :
  File Name   : level1-xx61.bix
Console#
```

TFTP Configuration Commands

ip tftp retry This command specifies the number of times the switch can retry transmitting a request to a TFTP server after waiting for the configured timeout period and receiving no response. Use the **no** form to restore the default setting.

Syntax

ip tftp retry *retries*

no ip tftp retry

retries - The number of times the switch can resend a request to a TFTP server before it aborts the connection. (Range: 1-16)

Default Setting

15

Command Mode

Global Configuration

Example

```
Console(config)#ip tftp retry 10
Console(config)#
```


ip tftp timeout This command specifies the time the switch can wait for a response from a TFTP server before retransmitting a request or timing out for the last retry. Use the **no** form to restore the default setting.

Syntax

ip tftp timeout *seconds*

no ip tftp timeout

seconds - The the time the switch can wait for a response from a TFTP server before retransmitting a request or timing out. (Range: 1-65535 seconds)

Default Setting

5 seconds

Command Mode

Global Configuration

Example

```
Console(config)#ip tftp timeout 10
Console(config)#
```

show ip tftp This command displays information about the TFTP settings configured on this switch.

Syntax

show ip tftp

Command Mode

Privileged Exec

Example

```
Console#show ip tftp
TFTP Settings:
  Retries : 15
  Timeout : 5 seconds
Console#
```

Line

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 18: Line Commands

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

* These commands only apply to the serial port.

line This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {console | vty}

console - Console terminal line.

vtty - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as “VTY” in screen displays such as [show users](#). However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

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

Related Commands

[show line \(124\)](#)

[show users \(97\)](#)

databits This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {7 | 8}

no databits

7 - Seven data bits per character.

8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

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

Related Commands

[parity \(118\)](#)

exec-timeout This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]

no exec-timeout

seconds - Integer that specifies the timeout interval.
(Range: 60 - 65535 seconds; 0: no timeout)

Default Setting

10 minutes

Command Mode

Line Configuration

Command Usage

- ◆ If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- ◆ This command applies to both the local console and Telnet connections.
- ◆ The timeout for Telnet cannot be disabled.
- ◆ Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

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

login This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the [username](#) command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- ◆ There are three authentication modes provided by the switch itself at login:
 - **login** selects authentication by a single global password as specified by the [password](#) line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
 - **login local** selects authentication via the user name and password specified by the [username](#) command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
 - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- ◆ This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

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

Related Commands

[username \(201\)](#)

[password \(118\)](#)

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

Syntax

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

no parity

none - No parity

even - Even parity

odd - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

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

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

Syntax

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

no password

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

password - Character string that specifies the line password.

(Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- ◆ When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the [password-thresh](#) command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- ◆ The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file from an FTP/SFTP server during system bootup. There is no need for you to manually configure encrypted passwords.

Example

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

Related Commands

[login \(117\)](#)

[password-thresh \(119\)](#)

password-thresh This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]

no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the [silent-time](#) command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

Example

To set the password threshold to five attempts, enter this command:

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

Related Commands

[silent-time \(120\)](#)

silent-time This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the [password-thresh](#) command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response.
(Range: 0-65535; where 0 means disabled)

Default Setting

Disabled

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

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

Related Commands

[password-thresh \(119\)](#)

speed This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*

no speed

bps - Baud rate in bits per second.

(Options: 9600, 19200, 38400, 57600, 115200 bps)

Default Setting

115200 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

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

stopbits This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

no stopbits

1 - One stop bit

2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

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

timeout login response This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

Syntax

timeout login response [*seconds*]

no timeout login response

seconds - Integer that specifies the timeout interval.
(Range: 10 - 300 seconds)

Default Setting

300 seconds

Command Mode

Line Configuration

Command Usage

- ◆ If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- ◆ This command applies to both the local console and Telnet connections.
- ◆ The timeout for Telnet cannot be disabled.
- ◆ Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

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

disconnect This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection.
(Range: 0-8)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```

Console#disconnect 1
Console#

```

Related Commands

[show ssh \(243\)](#)

[show users \(97\)](#)

terminal This command configures terminal settings, including escape-character, lines displayed, terminal type, width, and command history. Use the **no** form with the appropriate keyword to restore the default setting.

Syntax

```

terminal {escape-character {ascii-number | character} | history [size size] |
length length | terminal-type {ansi-bbs | vt-100 | vt-102} | width width}

```

escape-character - The keyboard character used to escape from current line input.

ascii-number - ASCII decimal equivalent. (Range: 0-255)

character - Any valid keyboard character.

history - The number of lines stored in the command buffer, and recalled using the arrow keys. (Range: 0-256)

length - The number of lines displayed on the screen. (Range: 24-200, where 0 means not to pause)

terminal-type - The type of terminal emulation used.

ansi-bbs - ANSI-BBS

vt-100 - VT-100

vt-102 - VT-102

width - The number of character columns displayed on the terminal. (Range: 0-80)

Default Setting

Escape Character: 27 (ASCII-number)

History: 10

Length: 24

Terminal Type: VT100
Width: 80

Command Mode

Privileged Exec

Example

This example sets the number of lines displayed by commands with lengthy output such as [show running-config](#) to 48 lines.

```
Console#terminal length 48  
Console#
```

show line This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line  
Terminal Configuration for this session:  
Length                : 24  
Width                 : 80  
History Size          : 10  
Escape Character(ASCII-number) : 27  
Terminal Type         : VT100  
  
Console Configuration:  
Password Threshold    : 3 times  
EXEC Timeout          : 600 seconds  
Login Timeout         : 300 seconds  
Silent Time           : Disabled  
Baud Rate             : 115200  
Data Bits             : 8  
Parity                : None  
Stop Bits             : 1  
  
VTY Configuration:  
Password Threshold    : 3 times  
EXEC Timeout          : 600 seconds
```

```
Login Timeout      : 300 sec.
Silent Time       : Disabled
Console#
```

Event Logging

This section describes commands used to configure event logging on the switch. To configure sending event logs as alerts using an SMTP mail server refer to [“SMTP Alerts” on page 132](#).

Table 19: Event Logging Commands

Command	Function	Mode
logging command	Stores CLI command execution records in syslog RAM and flash	GC
logging facility	Sets the facility type for remote logging of syslog messages	GC
logging history	Limits syslog messages saved to switch memory based on severity	GC
logging host	Adds a syslog server host IP address that will receive logging messages	GC
logging on	Controls logging of error messages	GC
logging sendmail	See “SMTP Alerts” on page 132	GC
logging trap	Limits syslog messages saved to a remote server based on severity	GC
clear log	Clears messages from the logging buffer	PE
show log	Displays log messages	PE
show logging	Displays the state of logging	PE

logging command This command stores CLI command execution records in syslog RAM and flash. Use the **no** form to disable this feature.

Syntax

[no] logging command

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The records stored include the commands executed from the CLI, command execution time and information about the CLI user including user name, user

interface (console, Telnet, SSH) and user IP address. The severity level for this record type is 6 (see the [logging facility](#) command).

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging facility This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

logging facility *type*

no logging facility

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging history This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*

no logging history {**flash** | **ram**}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

level - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 20: Logging Levels

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

Default Setting

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

logging host *host-ip-address* [**port** *udp-port*]

no logging host *host-ip-address*

host-ip-address - The IPv4 or IPv6 address of a syslog server.

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

Default Setting

UPD Port: 514

Command Mode

Global Configuration

Command Usage

- ◆ Use this command more than once to build up a list of host IP addresses.
- ◆ The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3  
Console(config)#
```

logging on This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

[no] logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the [logging history](#) command to control the type of error messages that are stored in memory. You can use the [logging trap](#) command to control the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on  
Console(config)#
```

Related Commands

[logging history \(126\)](#)

[logging trap \(129\)](#)

[clear log \(129\)](#)

logging trap This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

Syntax

logging trap [**level** *level*]

no logging trap [**level**]

level - One of the syslog severity levels listed in the table on [page 126](#).
Messages sent include the selected level through level 0.

Default Setting

Disabled
Level 7

Command Mode

Global Configuration

Command Usage

- ◆ Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- ◆ Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

Example

```
Console(config)#logging trap level 4  
Console(config)#
```

clear log This command clears messages from the log buffer.

Syntax

clear log [**flash** | **ram**]

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear log
Console#
```

Related Commands

[show log \(130\)](#)

show log This command displays the log messages stored in local memory.

Syntax

show log {flash | ram}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).
- ◆ All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

Example

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
    "VLAN 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
    "Unit 1, Port 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
Console#
```

show logging This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

show logging {command | flash | ram | sendmail | trap}

command - Stores CLI command execution records in syslog RAM and flash.

flash - Displays settings for storing event messages in flash memory (i.e., permanent memory).

ram - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

sendmail - Displays settings for the SMTP event handler ([page 135](#)).

trap - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), and the message level for RAM is “debugging” (i.e., default level 7 - 0).

```
Console#show logging flash
Global Configuration:
  Syslog Logging      : Enabled
Flash Logging Configuration:
  History Logging in Flash : Level Errors (3)
Console#show logging ram
Global Configuration:
  Syslog Logging      : Enabled
Ram Logging Configuration:
  History Logging in RAM  : Level Debugging (7)
Console#
```

Table 21: show logging flash/ram - display description

Field	Description
Syslog Logging	Shows if system logging has been enabled via the logging on command.
History Logging in Flash	The message level(s) reported based on the logging history command.
History Logging in RAM	The message level(s) reported based on the logging history command.

The following example displays settings for the trap function.

```
Console#show logging trap
Global Configuration:
  Syslog Logging      : Enabled
Remote Logging Configuration:
  Status              : Disabled
  Facility Type       : Local use 7 (23)
  Level Type          : Debugging messages (7)
Console#
```

Table 22: show logging trap - display description

Field	Description
<i>Global Configuration</i>	
Syslog logging	Shows if system logging has been enabled via the logging on command.
<i>Remote Logging Configuration</i>	
Status	Shows if remote logging has been enabled via the logging trap command.
Facility Type	The facility type for remote logging of syslog messages as specified in the logging facility command.
Level Type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.

Related Commands

[show logging sendmail \(135\)](#)

SMTP Alerts

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients. To configure event logging refer to [“Event Logging” on page 125](#).

Table 23: Event Logging Sendmail Commands

Command	Function	Mode
logging sendmail	Enables SMTP event handling	GC
logging sendmail destination-email	Email recipients of alert messages	GC
logging sendmail host	SMTP servers to receive alert messages	GC
logging sendmail level	Severity threshold used to trigger alert messages	GC
logging sendmail source-email	Email address used for “From” field of alert messages	GC
show logging sendmail	Displays SMTP event handler settings	NE, PE

logging sendmail This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[no] logging sendmail

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

logging sendmail destination-email This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[no] logging sendmail destination-email *email-address*

email-address - The source email address used in alert messages.
(Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail host This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[no] logging sendmail host *ip-address*

ip-address - IPv4 address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ You can specify up to three SMTP servers for event handling. However, you must enter a separate command to specify each server.
- ◆ To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- ◆ To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level This command sets the severity threshold used to trigger alert messages. Use the **no** form to restore the default setting.

Syntax

[no] logging sendmail level *level*

level - One of the system message levels ([page 126](#)). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages. Use the **no** form to restore the default value.

Syntax

logging sendmail source-email *email-address*

no logging sendmail source-email

email-address - The source email address used in alert messages.
(Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Privileged Exec

Example

```

Console#show logging sendmail
SMTP Servers
-----
 1. 10.20.1.2
 2. 10.1.2.1

SMTP Minimum Severity Level: 5

SMTP Destination E-mail Addresses
-----
 1. karl@email.com
 2. noc_team@email.com

SMTP Source E-mail Address:  switch99@email.com

SMTP Status:                  Enabled
Console#

```

Time

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.



Caution: It is strongly advised to use SNTP or NTP to maintain an accurate record of switch events. Manually setting the system clock can result in an inaccurate time-stamp on system events.

Table 24: Time Commands

Command	Function	Mode
<i>SNTP Commands</i>		
<code>sntp client</code>	Accepts time from specified time servers	GC
<code>sntp poll</code>	Sets the interval at which the client polls for time	GC
<code>sntp server</code>	Specifies one or more time servers	GC
<code>show sntp</code>	Shows current SNTP configuration settings	NE, PE
<i>NTP Commands</i>		
<code>ntp authenticate</code>	Enables authentication for NTP traffic	GC
<code>ntp authentication-key</code>	Configures authentication keys	GC
<code>ntp client</code>	Enables the NTP client for time updates from specified servers	GC
<code>ntp server</code>	Specifies NTP servers to poll for time updates	GC
<code>show ntp</code>	Shows current NTP configuration settings	NE, PE

Table 24: Time Commands (Continued)

Command	Function	Mode
<i>Manual Configuration Commands</i>		
<code>clock summer-time (date)</code>	Configures summer time* for the switch's internal clock	GC
<code>clock summer-time (predefined)</code>	Configures summer time* for the switch's internal clock	GC
<code>clock summer-time (recurring)</code>	Configures summer time* for the switch's internal clock	GC
<code>clock timezone</code>	Sets the time zone for the switch's internal clock	GC
<code>calendar set</code>	Sets the system date and time	PE
<code>show calendar</code>	Displays the current date and time setting	NE, PE

* Daylight savings time.

SNTP Commands

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

Syntax

[no] sntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (e.g., Dec 31 07:32:04 2014).
- ◆ This command enables client time requests to time servers specified via the `sntp server` command. It issues time synchronization requests based on the interval set via the `sntp poll` command.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current Time: Dec 23 02:52:44 2015
Poll Interval: 60
Current Mode: Unicast
```

```
SNTP Status : Enabled
SNTP Server 137.92.140.80 0.0.0.0 0.0.0.0
Current Server: 137.92.140.80
Console#
```

Related Commands

[sntp server \(138\)](#)

[sntp poll \(138\)](#)

[show sntp \(139\)](#)

sntp poll This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*

no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Example

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

Related Commands

[sntp client \(137\)](#)

sntp server This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the **no** form to clear all time servers from the current list, or to clear a specific server.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

no sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IPv4 or IPv6 address of a time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the [sntp poll](#) command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands[sntp client \(137\)](#)[sntp poll \(138\)](#)[show sntp \(139\)](#)

show sntp This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

Example

```
Console#show sntp
Current Time   : Nov  5 18:51:22 2015
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80
                : 137.92.140.90
                : 137.92.140.99
Current Server : 137.92.140.80
Console#
```

NTP Commands

ntp authenticate This command enables authentication for NTP client-server communications. Use the **no** form to disable authentication.

Syntax

[no] ntp authenticate

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

Example

```
Console(config)#ntp authenticate
Console(config)#
```

Related Commands

[ntp authentication-key \(140\)](#)

ntp authentication-key This command configures authentication keys and key numbers to use when NTP authentication is enabled. Use the **no** form of the command to clear a specific authentication key or all keys from the current list.

Syntax

ntp authentication-key *number* **md5** *key*

no ntp authentication-key [*number*]

number - The NTP authentication key ID number. (Range: 1-65535)

md5 - Specifies that authentication is provided by using the message digest algorithm 5.

key - An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The key number specifies a key value in the NTP authentication key list. Up to 255 keys can be configured on the switch. Re-enter this command for each server you want to configure.
- ◆ Note that NTP authentication key numbers and values must match on both the server and client.
- ◆ NTP authentication is optional. When enabled with the **ntp authenticate** command, you must also configure at least one key number using this command.
- ◆ Use the **no** form of this command without an argument to clear all authentication keys in the list.

Example

```
Console(config)#ntp authentication-key 45 md5 thisiskey45  
Console(config)#
```

Related Commands

[ntp authenticate \(140\)](#)

ntp client This command enables NTP client requests for time synchronization from NTP time servers specified with the **ntp servers** command. Use the **no** form to disable NTP client requests.

Syntax

[no] ntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The SNTP and NTP clients cannot be enabled at the same time. First disable the SNTP client before using this command.
- ◆ The time acquired from time servers is used to record accurate dates and times for log events. Without NTP, the switch only records the time starting from the factory default set at the last bootup (e.g., Dec 10 16:04:43 2014).

- ◆ This command enables client time requests to time servers specified via the **ntp servers** command. It issues time synchronization requests based on the interval set via the **ntp poll** command.

Example

```
Console(config)#ntp client
Console(config)#
```

Related Commands

[sntp client \(137\)](#)

[ntp server \(142\)](#)

ntp server This command sets the IP addresses of the servers to which NTP time requests are issued. Use the **no** form of the command to clear a specific time server or all servers from the current list.

Syntax

ntp server *ip-address* [**key** *key-number*]

no ntp server [*ip-address*]

ip-address - IP address of an NTP time server.

key-number - The number of an authentication key to use in communications with the server. (Range: 1-65535)

Default Setting

Version number: 3

Command Mode

Global Configuration

Command Usage

- ◆ This command specifies time servers that the switch will poll for time updates when set to NTP client mode. It issues time synchronization requests based on the interval set with the **ntp poll** command. The client will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- ◆ You can configure up to 50 NTP servers on the switch. Re-enter this command for each server you want to configure.
- ◆ NTP authentication is optional. If enabled with the **ntp authenticate** command, you must also configure at least one key number using the **ntp authentication-key** command.
- ◆ Use the **no** form of this command without an argument to clear all configured servers in the list.

Example

```

Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#

```

Related Commands

[ntp client \(141\)](#)

[show ntp \(143\)](#)

show ntp This command displays the current time and configuration settings for the NTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current NTP mode (i.e., unicast).

Example

```

Console#show ntp
Current Time           : Apr 29 13:57:32 2015
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status             : Disabled
NTP Authenticate Status : Enabled
Last Update NTP Server : 0.0.0.0      Port: 0
Last Update Time       : Jan  1 00:00:00 1970 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885
Console#

```

Manual Configuration Commands

clock summer-time (date) This command sets the start, end, and offset times of summer time (daylight savings time) for the switch on a one-time basis. Use the **no** form to disable summer time.

Syntax

clock summer-time *name* **date** *b-date b-month b-year b-hour b-minute e-date e-month e-year e-hour e-minute [offset]*

no clock summer-time

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

b-date - Day of the month when summer time will begin. (Range: 1-31)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-year - The year summer time will begin.

b-hour - The hour summer time will begin. (Range: 0-23 hours)

b-minute - The minute summer time will begin. (Range: 0-59 minutes)

e-date - Day of the month when summer time will end. (Range: 1-31)

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

e-year - The year summer time will end.

e-hour - The hour summer time will end. (Range: 0-23 hours)

e-minute - The minute summer time will end. (Range: 0-59 minutes)

offset - Summer time offset from the regular time zone, in minutes.
(Range: 1-120 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- ◆ This command sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone (that is, the offset).

Example

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

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


Related Commands[show sntp \(139\)](#)

clock summer-time (predefined) This command configures the summer time (daylight savings time) status and settings for the switch using predefined configurations for several major regions in the world. Use the **no** form to disable summer time.

Syntax

clock summer-time *name* **predefined** [**australia** | **europe** | **new-zealand** | **usa**]

no clock summer-time

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- ◆ This command sets the summer-time time relative to the configured time zone. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time time zone appropriate for your location, or manually configure summer time if these predefined configurations do not apply to your location (see [clock summer-time \(date\)](#) or [clock summer-time \(recurring\)](#)).

Table 25: Predefined Summer-Time Parameters

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

Example

The following example sets the Summer Time setting to use the predefined settings for the European region.

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

Related Commands

[show sntp \(139\)](#)

clock summer-time (recurring) This command allows the user to manually configure the start, end, and offset times of summer time (daylight savings time) for the switch on a recurring basis. Use the **no** form to disable summer-time.

Syntax

clock summer-time *name recurring b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute [offset]*

no clock summer-time

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

b-week - The week of the month when summer time will begin. (Range: 1-5)

b-day - The day of the week when summer time will begin. (Options: **sunday | monday | tuesday | wednesday | thursday | friday | saturday**)

b-month - The month when summer time will begin. (Options: **january | february | march | april | may | june | july | august | september | october | november | december**)

b-hour - The hour when summer time will begin. (Range: 0-23 hours)

b-minute - The minute when summer time will begin. (Range: 0-59 minutes)

e-week - The week of the month when summer time will end. (Range: 1-5)

e-day - The day of the week summer time will end. (Options: **sunday | monday | tuesday | wednesday | thursday | friday | saturday**)

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

e-hour - The hour when summer time will end. (Range: 0-23 hours)

e-minute - The minute when summer time will end. (Range: 0-59 minutes)

offset - Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- ◆ This command sets the summer-time time zone relative to the currently configured time zone. To display a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone (that is, the offset).

Example

The following example sets a recurring 60 minute offset summer-time to begin on the Friday of the 1st week of March at 01:59 hours and summer time to end on the Saturday of the 2nd week of November at 01:59 hours.

```
Console(config)#clock summer-time MESZ recurring 1 friday march 01 59 3
saturday november 1 59 60
Console(config)#
```

Related Commands

[show sntp \(139\)](#)

clock timezone This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes*
{**before-utc** | **after-utc**}

name - Name of timezone, usually an acronym. (Range: 1-30 characters)

hours - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)

minutes - Number of minutes before/after UTC. (Range: 0-59 minutes)

before-utc - Sets the local time zone before (east) of UTC.

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

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

Related Commands

[show sntp \(139\)](#)

calendar set This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec {day month year | month day year}*

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

min - Minute. (Range: 0 - 59)

sec - Second. (Range: 0 - 59)

day - Day of month. (Range: 1 - 31)

month - **january | february | march | april | may | june | july | august | september | october | november | december**

year - Year (4-digit). (Range: 1970 - 2037)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Note that when SNTP is enabled, the system clock cannot be manually configured.

Example

This example shows how to set the system clock to 10:30:36, July 29th, 2018,.

```
Console#calendar set 10 30 36 29 July 2018
Console#
```

show calendar This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar
Current Time       : May 13 14:08:18 2014
Time Zone         : UTC, 08:00
Summer Time       : Not configured
Summer Time in Effect : No
Console#
```

Time Range

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

Table 26: Time Range Commands

Command	Function	Mode
time-range	Specifies the name of a time range, and enters time range configuration mode	GC
absolute	Sets the absolute time range for the execution of a command	TR
periodic	Sets the time range for the periodic execution of a command	TR
show time-range	Shows configured time ranges.	PE

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

Syntax

[no] time-range *name*

name - Name of the time range. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ This command sets a time range for use by other functions, such as Access Control Lists.
- ◆ A maximum of eight rules can be configured for a time range.

Example

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

Related Commands

[Access Control Lists \(325\)](#)

absolute This command sets the absolute time range for the execution of a command. Use the **no** form to remove a previously specified time.

Syntax

absolute start *hour minute day month year*
[**end** *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

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

minute - Minute. (Range: 0-59)

day - Day of month. (Range: 1-31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** |
september | **october** | **november** | **december**

year - Year (4-digit). (Range: 2013-2037)

Default Setting

None

Command Mode

Time Range Configuration

Command Usage

- ◆ If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.
- ◆ If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

Example

This example configures the time for the single occurrence of an event.

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april
2009
Console(config-time-range)#
```

periodic This command sets the time range for the periodic execution of a command. Use the **no** form to remove a previously specified time range.

Syntax

[no] periodic {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend} hour minute to {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend} hour minute

daily - Daily

friday - Friday

monday - Monday

saturday - Saturday

sunday - Sunday

thursday - Thursday

tuesday - Tuesday

wednesday - Wednesday

weekdays - Weekdays

weekend - Weekends

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

minute - Minute. (Range: 0-59)

Default Setting

None

Command Mode

Time Range Configuration

Command Usage

- ◆ If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.
- ◆ If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

Example

This example configures a time range for the periodic occurrence of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

show time-range This command shows configured time ranges.

Syntax

show time-range [*name*]

name - Name of the time range. (Range: 1-32 characters)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show time-range r&d
Time-range r&d:
  status: inactive
  absolute start 01:01 01 April 2015
  periodic    Daily 01:01 to    Daily 02:01
  periodic    Daily 02:01 to    Daily 03:01
Console#
```

Switch Clustering

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Table 27: Switch Cluster Commands

Command	Function	Mode
cluster	Configures clustering on the switch	GC
cluster commander	Configures the switch as a cluster Commander	GC
cluster ip-pool	Sets the cluster IP address pool for Members	GC
cluster member	Sets Candidate switches as cluster members	GC
rcommand	Provides configuration access to Member switches	PE

Table 27: Switch Cluster Commands (Continued)

Command	Function	Mode
show cluster	Displays the switch clustering status	PE
show cluster members	Displays current cluster Members	PE
show cluster candidates	Displays current cluster Candidates in the network	PE

Using Switch Clustering

- ◆ A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage the Member switches through the cluster’s “internal” IP addresses.
- ◆ Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- ◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.
- ◆ The cluster VLAN 4093 is not configured by default. Before using clustering, take the following actions to set up this VLAN:
 1. Create VLAN 4093 (see [“Editing VLAN Groups” on page 461](#)).
 2. Add the participating ports to this VLAN (see [“Configuring VLAN Interfaces” on page 463](#)), and set them to hybrid mode, tagged members, PVID = 1, and acceptable frame type = all.



Note: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the [rcommand](#) to connect to the Member switch.

cluster This command enables clustering on the switch. Use the **no** form to disable clustering.

Syntax

[no] cluster

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ To create a switch cluster, first be sure that clustering is enabled on the switch (the default is disabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- ◆ Switch clusters are limited to the same Ethernet broadcast domain.
- ◆ There can be up to 100 candidates and 36 member switches in one cluster.
- ◆ A switch can only be a Member of one cluster.
- ◆ Configured switch clusters are maintained across power resets and network changes.

Example

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

cluster commander This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

Syntax

[no] cluster commander

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

- ◆ Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the **rcommand id** command to connect to the Member switch.

Example

```
Console(config)#cluster commander  
Console(config)#
```

cluster ip-pool This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

Syntax

cluster ip-pool *ip-address*

no cluster ip-pool

ip-address - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

Default Setting

10.254.254.1

Command Mode

Global Configuration

Command Usage

- ◆ An “internal” IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.*member-ID*. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.
- ◆ Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- ◆ You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

Example

```
Console(config)#cluster ip-pool 10.2.3.4  
Console(config)#
```

cluster member This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

Syntax

cluster member mac-address *mac-address* **id** *member-id*

no cluster member id *member-id*

mac-address - The MAC address of the Candidate switch.

member-id - The ID number to assign to the Member switch. (Range: 1-36)

Default Setting

No Members

Command Mode

Global Configuration

Command Usage

- ◆ The maximum number of cluster Members is 36.
- ◆ The maximum number of cluster Candidates is 100.

Example

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

rcommand This command provides access to a cluster Member CLI for configuration.

Syntax

rcommand id *member-id*

member-id - The ID number of the Member switch. (Range: 1-36)

Command Mode

Privileged Exec

Command Usage

- ◆ This command only operates through a Telnet connection to the Member switch. Managing cluster Members using the local console CLI on the Commander is not supported.
- ◆ There is no need to enter the username and password for access to the Member switch CLI.

Example

```
Console#rcommand id 1

      CLI session with the GEL-2861 is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

show cluster This command shows the switch clustering configuration.

Command Mode

Privileged Exec

Example

```
Console#show cluster
Role           : commander
Interval Heartbeat : 30
Heartbeat Loss Count : 3 seconds
Number of Members   : 1
Number of Candidates : 2
Console#
```

show cluster members This command shows the current switch cluster members.

Command Mode

Privileged Exec

Example

```
Console#show cluster members
Cluster Members:
ID           : 1
Role         : Active member
IP Address   : 10.254.254.2
MAC Address  : 00-E0-0C-00-00-FE
Description  : GEL-2861
Console#
```

show cluster candidates This command shows the discovered Candidate switches in the network.

Command Mode
Privileged Exec

Example

```
Console#show cluster candidates
Cluster Candidates:
Role           MAC Address      Description
-----
Candidate join 00-E0-0C-00-00-FE GEL-2861
Candidate      00-12-CF-0B-47-A0 GEL-2861
Console#
```

SNMP Commands

SNMP commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 28: SNMP Commands

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

Table 28: SNMP Commands (Continued)

Command	Function	Mode
<code>show snmp engine-id</code>	Shows the SNMP engine ID	PE
<code>show snmp group</code>	Shows the SNMP groups	PE
<code>show snmp user</code>	Shows the SNMP users	PE
<code>show snmp view</code>	Shows the SNMP views	PE
<i>Notification Log Commands</i>		
<code>nlm</code>	Enables the specified notification log	GC
<code>snmp-server notify-filter</code>	Creates a notification log and specifies the target host	GC
<code>show nlm oper-status</code>	Shows operation status of configured notification logs	PE
<code>show snmp notify-filter</code>	Displays the configured notification logs	PE
<i>Transceiver Power Threshold Trap Commands</i>		
<code>transceiver-threshold current</code>	Sends a trap when the transceiver current falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold rx-power</code>	Sends a trap when the power level of the received signal falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold temperature</code>	Sends a trap when the transceiver temperature falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold tx-power</code>	Sends a trap when the power level of the transmitted signal power outside the specified thresholds	IC (Port)
<code>transceiver-threshold voltage</code>	Sends a trap when the transceiver voltage falls outside the specified thresholds	IC (Port)
<i>Additional Trap Commands</i>		
<code>memory</code>	Sets the rising and falling threshold for the memory utilization alarm	GC
<code>process cpu</code>	Sets the rising and falling threshold for the CPU utilization alarm	GC
<code>process cpu guard</code>	Sets the CPU utilization watermark and threshold	GC
<code>show memory</code>	Shows memory utilization parameters	PE
<code>show process cpu</code>	Shows CPU utilization parameters	NE, PE
<code>show process cpu guard</code>	Shows the CPU utilization watermark and threshold	PE
<code>show process cpu task</code>	Shows CPU utilization per process	NE, PE

General SNMP Commands

snmp-server This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[no] snmp-server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

snmp-server community This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

string - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive;
Maximum number of strings: 5)

ro - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- ◆ **public** - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- ◆ **private** - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

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

Syntax

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

[snmp-server location \(162\)](#)

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

Syntax

snmp-server location *text*

no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

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

Related Commands

[snmp-server contact \(162\)](#)

show snmp This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counters for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
  Authentication : Enabled
  MAC-notification : Disabled
  MAC-notification interval : 1 second(s)

SNMP Communities :
  1. public, and the access level is read-only
  2. private, and the access level is read/write

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
```

```
SNMP Logging: Disabled  
Console#
```

SNMP Target Host Commands

snmp-server enable traps This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[no] snmp-server enable traps [authentication | mac-notification [interval seconds]]

authentication - Keyword to issue authentication failure notifications.

mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

interval - Specifies the interval between issuing two consecutive traps. (Range: 1-3600 seconds; Default: 1 second)

Default Setting

Issue authentication traps
Other traps are disabled

Command Mode

Global Configuration

Command Usage

- ◆ If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- ◆ The **snmp-server enable traps** command is used in conjunction with the [snmp-server host](#) command. Use the [snmp-server host](#) command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one [snmp-server host](#) command.
- ◆ The authentication traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the [snmp-server group](#) command.
- ◆ For mac-notification, when there is a MAC-address-table change, it will be stored in buffer first. If the interval time is set, any changes stored in the buffer will be sent continuously until the buffer is empty. If after sending the buffer

data, the interval time has not been reached, address table changes will be kept in the buffer, and this new buffer data will be sent once the interval time expires.

For example: if the trap interval is set for 15 minutes and the MAC-address table data is sent at 10:00. At 10:15 data sent will be the buffer data composed of new dynamic MAC data collected since the original MAC-address-table data was sent at 10:00. Therefore at 10:30 and the following 15 minute intervals, only changes gathered in the buffer since the previous transmission will be sent.

Example

```
Console(config)#snmp-server enable traps authentication
Console(config)#
```

Related Commands

[snmp-server host \(165\)](#)

snmp-server host This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]]
community-string [**version** {1 | 2c | 3 {**auth** | **noauth** | **priv**} [**udp-port** *port*]}]

no snmp-server host *host-addr*

host-addr - IPv4 or IPv6 address of the host (the targeted recipient).
(Maximum host addresses: 5 trap destination IP address entries)

inform - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

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

seconds - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

community-string - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend defining it with the [snmp-server community](#) command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

version - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

auth | noauth | priv - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” in the *Web Management Guide* for further information about these authentication and encryption options.

port - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

Host Address: None

Notification Type: Traps

SNMP Version: 1

UDP Port: 162

Command Mode

Global Configuration

Command Usage

- ◆ If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- ◆ The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- ◆ Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- ◆ Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent ([page 161](#)).
2. Create a view with the required notification messages ([page 173](#)).
3. Create a group that includes the required notify view ([page 170](#)).

4. Allow the switch to send SNMP traps; i.e., notifications ([page 164](#)).
5. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent ([page 161](#)).
 2. Create a remote SNMPv3 user to use in the message exchange process ([page 171](#)).
 3. Create a view with the required notification messages ([page 173](#)).
 4. Create a group that includes the required notify view ([page 170](#)).
 5. Allow the switch to send SNMP traps; i.e., notifications ([page 164](#)).
 6. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
- ◆ The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
 - ◆ If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the [snmp-server user](#) command. Otherwise, an SNMPv3 group will be automatically created by the **snmp-server host** command using the name of the specified community string, and default settings for the read, write, and notify view.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

[snmp-server enable traps \(164\)](#)

snmp-server enable port-traps link-up-down

This command enables the device to send SNMP traps (i.e., SNMP notifications) when a link-up or link-down state change occurs. Use the **no** form to restore the default setting.

Syntax

[no] snmp-server enable port-traps link-up-down

link-up-down - Keyword to issue trap when a link-up or link-down state change occurs.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps link-up-down
Console(config)#
```

snmp-server enable port-traps mac-notification

This command enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed. Use the no form to restore the default setting.

Syntax

[no] snmp-server enable port-traps mac-notification

mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can enable MAC authentication traps on the current interface only if they are also enabled at the global level with the [snmp-server enable traps mac-authentication](#) command.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config)#
```

show snmp-server enable port-traps

This command shows if SNMP traps are enabled or disabled for the specified interfaces.

Syntax

show snmp-server enable port-traps interface *[interface]*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show snmp-server enable port-traps interface
Interface MAC Notification Trap
-----
Eth 1/1                                     No
Eth 1/2                                     No
Eth 1/3                                     No
:
```

SNMPv3 Commands

snmp-server engine-id This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*

no snmp-server engine-id {**local** | **remote** {*ip-address*}}

local - Specifies the SNMP engine on this switch.

remote - Specifies an SNMP engine on a remote device.

ip-address - IPv4 or IPv6 address of the remote device.

engineid-string - String identifying the engine ID. (Range: 9-64 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- ◆ An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- ◆ A remote engine ID is required when using SNMPv3 informs. (See the [snmp-server host](#) command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine

ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

- ◆ Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.
- ◆ A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users ([page 171](#)).

Example

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

Related Commands

[snmp-server host](#) (165)

snmp-server group This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

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

```
no snmp-server group groupname
```

groupname - Name of an SNMP group. (Range: 1-32 characters)

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" in the *Web Management Guide* for further information about these authentication and encryption options.

readview - Defines the view for read access. (1-32 characters)

writeview - Defines the view for write access. (1-32 characters)

notifyview - Defines the view for notifications. (1-32 characters)

Default Setting

Default groups: public¹ (read only), private² (read/write)

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

writeview - Nothing is defined.

notifyview - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- ◆ A group sets the access policy for the assigned users.
- ◆ When authentication is selected, the MD5 or SHA algorithm is used as specified in the `snmp-server user` command.
- ◆ When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- ◆ For additional information on the notification messages supported by this switch, see table for “Supported Notification Messages” in the *Web Management Guide*. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the `snmp-server enable traps` command.

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

snmp-server user This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username* *groupname*
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv** {**3des** | **aes128** | **aes192** | **aes256** | **des56**} *priv-password*]]

snmp-server user *username* *groupname* **remote** *ip-address*
{**v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv** {**3des** | **aes128** | **aes192** | **aes256** | **des56**} *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote** *ip-address* **v3**}

username - Name of user connecting to the SNMP agent.
(Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned.
(Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - IPv4 address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

1. No view is defined.
2. Maps to the defaultview.

auth - Uses SNMPv3 with authentication.

md5 | **sha** - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (Range: 8-32 characters for unencrypted password.)

If the **encrypted** option is selected, enter an encrypted password. (Range: 32 characters for MD5 encrypted password, 40 characters for SHA encrypted password)

3des - Uses SNMPv3 with privacy with 3DES (168-bit) encryption.

aes128 - Uses SNMPv3 with privacy with AES128 encryption.

aes192 - Uses SNMPv3 with privacy with AES192 encryption.

aes256 - Uses SNMPv3 with privacy with AES256 encryption.

des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (Range: 8-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- ◆ Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.
- ◆ The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the [snmp-server engine-id](#) command before using this configuration command.
- ◆ Before you configure a remote user, use the [snmp-server engine-id](#) command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- ◆ SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore

need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve r&d v3 auth md5 greenpeace priv des56
einstien
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#snmp-server user mark r&d remote 192.168.1.19 v3 auth md5
greenpeace priv des56 einstien
Console(config)#
```

snmp-server view This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

view-name - Name of an SNMP view. (Range: 1-32 characters)

oid-tree - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

included - Defines an included view.

excluded - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- ◆ Views are used in the [snmp-server group](#) command to restrict user access to specified portions of the MIB tree.
- ◆ The predefined view "defaultview" includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in the following table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp engine-id This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

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

Table 29: show snmp engine-id - display description

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

show snmp group Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```

Console#show snmp group
Group Name       : r&d
Security Model   : v3
Security Level   : Authentication and privacy
Read View        : No readview specified
Write View       : No writeview specified
Notify View      : No notifyview specified
Storage Type     : Nonvolatile
Row Status       : Active

Group Name       : public
Security Model   : v1
Read View        : defaultview
Write View       : No writeview specified
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active

Group Name       : public
Security Model   : v2c
Read View        : defaultview
Write View       : No writeview specified
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active

Group Name       : private
Security Model   : v1
Read View        : defaultview
Write View       : defaultview
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active

Group Name       : private
Security Model   : v2c
Read View        : defaultview
Write View       : defaultview
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active
Console#

```

Table 30: show snmp group - display description

Field	Description
Group Name	Name of an SNMP group.
Security Model	The SNMP version.
Security Level	This associated security level can use SNMPv3 with authentication, no authentication, or with authentication and privacy.

Table 30: show snmp group - display description (Continued)

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

show snmp user This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

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

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

Table 31: show snmp user - display description

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

Table 31: show snmp user - display description (Continued)

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

show snmp view This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```

Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name      : defaultview
Subtree OID    : 1
View Type      : included
Storage Type   : volatile
Row Status     : active
Console#

```

Table 32: show snmp view - display description

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

Notification Log Commands

nlm This command enables or disables the specified notification log.

Syntax

[no] nlm *filter-name*

filter-name - Notification log name. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Notification logging is enabled by default, but will not start recording information until a logging profile specified by the [snmp-server notify-filter](#) command is enabled by the **nlm** command.
- ◆ Disabling logging with this command does not delete the entries stored in the notification log.

Example

This example enables the notification log A1.

```
Console(config)#nlm A1  
Console(config)#
```

snmp-server notify-filter This command creates an SNMP notification log. Use the **no** form to remove this log.

Syntax

[no] snmp-server notify-filter *profile-name* **remote** *ip-address*

profile-name - Notification log profile name. (Range: 1-32 characters)

ip-address - IPv4 or IPv6 address of a remote device. The specified target host must already have been configured using the [snmp-server host](#) command.



Note: The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether there are Traps or Informs that may exceed retransmission limits. The Notification Log MIB (NLM,

RFC 3014) provides an infrastructure in which information from other MIBs may be logged.

- ◆ Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.
- ◆ If notification logging is not configured and enabled, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.
- ◆ To avoid this problem, notification logging should be configured and enabled using the **snmp-server notify-filter** command and **nlm** command, and these commands stored in the startup configuration file. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.
- ◆ When this command is executed, a notification log is created (with the default parameters defined in RFC 3014). Notification logging is enabled by default (see the **nlm** command), but will not start recording information until a logging profile specified with this command is enabled with the **nlm** command.
- ◆ Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information recorded in a notification log, and the entry aging time can only be configured using SNMP from a network management station.
- ◆ When a trap host is created with the **snmp-server host** command, a default notify filter will be created as shown in the example under the **show snmp notify-filter** command.

Example

This example first creates an entry for a remote host, and then instructs the switch to record this device as the remote host for the specified notification log.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

show nlm oper-status This command shows the operational status of configured notification logs.

Command Mode

Privileged Exec

Example

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

show snmp notify-filter This command displays the configured notification logs.

Command Mode

Privileged Exec

Example

This example displays the configured notification logs and associated target hosts.

```
Console#show snmp notify-filter
Filter profile name      IP address
-----
A1                      10.1.19.23
Console#
```

Additional Trap Commands

memory This command sets an SNMP trap based on configured thresholds for memory utilization. Use the **no** form to restore the default setting.

Syntax

memory {**rising** *rising-threshold* | **falling** *falling-threshold*}

no memory {**rising** | **falling**}

rising-threshold - Rising threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

Default Setting

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

Command Usage

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

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

Related Commands

[show memory \(90\)](#)

process cpu This command sets an SNMP trap based on configured thresholds for CPU utilization. Use the no form to restore the default setting.

Syntax

process cpu {*rising* *rising-threshold* | *falling* *falling-threshold*}

no process cpu {*rising* | *falling*}

rising-threshold - Rising threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

Default Setting

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

Command Usage

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

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

Related Commands

[show process cpu \(91\)](#)

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

Syntax

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

high-watermark - If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark. (Range: 40-100%)

low-watermark - If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark. (Range: 40-100%)

max-threshold - If the number of packets being processed per second by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold. (Range: 50-300 pps)

min-threshold - If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold. (Range: 50-300 pps)

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

Default Setting

Guard Status: Disabled

High Watermark: 90%

Low Watermark: 70%

Maximum Threshold: 500 packets per second

Minimum Threshold: 50 packets per second

Trap Status: Disabled

Command Mode

Global Configuration

Command Usage

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

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

Example

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

Related Commands

[show process cpu guard \(91\)](#)

Remote Monitoring Commands

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

Table 33: RMON Commands

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

rmon alarm This command sets threshold bounds for a monitored variable. Use the **no** form to remove an alarm.

Syntax

```
rmon alarm index variable interval {absolute | delta}
rising-threshold threshold [event-index] falling-threshold threshold
[event-index] [owner name]
```

```
no rmon alarm index
```

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

variable – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

interval – The polling interval. (Range: 1-31622400 seconds)

absolute – The variable is compared directly to the thresholds at the end of the sampling period.

delta – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

threshold – An alarm threshold for the sampled variable.
(Range: 0-2147483647)

event-index – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-32 characters)

Default Setting

1.3.6.1.4.1.259.10.1.43.104.1 - 1.3.6.1.4.1.259.10.1.43.102.26/

1.3.6.1.4.1.259.10.1.43.101.52

Taking delta samples every 30 seconds,

Rising threshold is 892800, assigned to event 0

Falling threshold is 446400, assigned to event 0

Command Mode

Global Configuration

Command Usage

- ◆ If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- ◆ If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be

generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.

- ◆ If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.

Example

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta
    rising-threshold 100 1 falling-threshold 30 1 owner mike
Console(config)#
```

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

Syntax

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

no rmon event *index*

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

log – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see [“Event Logging” on page 125](#)).

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

community – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the **rmon event** command by itself, it is recommended that the string be defined using the [snmp-server community](#) command prior to using the **rmon event** command. (Range: 1-32 characters)

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

name – Name of the person who created this entry. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- ◆ The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

Example

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history This command periodically samples statistics on a physical interface. Use the **no** form to disable periodic sampling.

Syntax

rmon collection history controlEntry *index*

[**buckets** *number* [**interval** *seconds*]] |

[**interval** *seconds*] |

[**owner** *name* [**buckets** *number* [**interval** *seconds*]]]

no rmon collection history controlEntry *index*

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

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

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

name – Name of the person who created this entry.
(Range: 1-32 characters)

Default Setting

1.3.6.1.4.1.259.10.1.43.104.1 - 1.3.6.1.4.1.259.10.1.43.104.102.26/

1.3.6.1.4.1.259.10.1.43.101.52

Buckets: 8

Interval: 30 seconds for even numbered entries,
1800 seconds for odd numbered entries

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

- ◆ The information collected for each sample includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.
- ◆ The switch reserves two controlEntry index entries for each port. If a default index entry is re-assigned to another port by this command, the **show running-config** command will display a message indicating that this index is not available for the port to which is normally assigned.

For example, if control entry 15 is assigned to port 5 as shown below, the **show running-config** command will indicate that this entry is not available for port 8.

```
Console(config)#interface ethernet 1/5
Console(config-if)#rmon collection history controlEntry 15
Console(config-if)#end
Console#show running-config
!
interface ethernet 1/5
  rmon collection history controlEntry 15 buckets 50 interval 1800
...
interface ethernet 1/8
  no rmon collection history controlEntry 15
```

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history controlentry 21 owner mike buckets
24 interval 60
Console(config-if)#
```

rmon collection rmon1 This command enables the collection of statistics on a physical interface. Use the **no rmon collection rmon1** form to disable statistics collection.

Syntax

rmon collection rmon1 controlEntry *index* [**owner** *name*]

no rmon collection rmon1 controlEntry *index*

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

name – Name of the person who created this entry.
(Range: 1-32 characters)

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- ◆ The information collected for each entry includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlentry 1 owner mike
Console(config-if)#
```

show rmon alarms This command shows the settings for all configured alarms.

Command Mode

Privileged Exec

Example

```
Console#show rmon alarms
Alarm 1 is valid, owned by
Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
Taking delta samples, last value was 0
Rising threshold is 892800, assigned to event 0
Falling threshold is 446400, assigned to event 0
:
```

show rmon events This command shows the settings for all configured events.

Command Mode

Privileged Exec

Example

```
Console#show rmon events
Event 2 is valid, owned by mike
Description is urgent
Event firing causes log and trap to community , last fired 00:00:00
Console#
```

show rmon history This command shows the sampling parameters configured for each entry in the history group.

Command Mode

Privileged Exec

Example

```
Console#show rmon history
Entry 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
Requested # of time intervals, ie buckets, is 8
Granted # of time intervals, ie buckets, is 8
Sample # 1 began measuring at 00:00:01
Received 77671 octets, 1077 packets,
61 broadcast and 978 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers packets,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Network utilization is estimated at 0
:
```

show rmon statistics This command shows the information collected for all configured entries in the statistics group.

Command Mode

Privileged Exec

Example

```
Console#show rmon statistics
Interface 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
Received 164289 octets, 2372 packets,
120 broadcast and 2211 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events (due to lack of resources): 0
# of packets received of length (in octets):
64: 2245, 65-127: 87, 128-255: 31,
256-511: 5, 512-1023: 2, 1024-1518: 2
:
```


Flow Sampling Commands

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



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

Table 34: sFlow Commands

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

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

Syntax

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

no sflow owner *owner-name*

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

timeout-value - The length of time the sFlow interface is available to send samples to a receiver, after which the owner and associated polling and

sampling data source instances are removed from the configuration.
(Range: 30-10000000 seconds)

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

ipv6-address - IPv6 address of the sFlow collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

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

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

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

Default Setting

No owner is configured

UDP Port: 6343

Version: v4

Maximum Datagram Size: 1400 bytes

Command Mode

Privileged Exec

Command Usage

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

Example

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

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

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

```
Console#sflow owner stat_server1 timeout 100 port 35100
Console#
```

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

Syntax

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

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

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

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

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

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

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

Default Setting

No sFlow polling instance is configured.

Command Mode

Privileged Exec

Command Usage

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

Example

This example sets the polling interval to 10 seconds.

```
Console#sflow polling interface ethernet 1/1 instance 1 receiver owner1
polling-interval 50
Console#
```

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

Syntax

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

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

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

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

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

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

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

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

Default Setting

No sFlow sampling instance id configured.

Maximum Header Size: 128 bytes

Command Mode

Privileged Exec

Example

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

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

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

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

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

Syntax

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

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

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

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

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

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

Console#
```


Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access³ to the data ports.

Table 35: Authentication Commands

Command Group	Function
User Accounts and Privilege Levels	Configures the basic user names and passwords for management access, and assigns a privilege level to specified command groups or individual commands
Authentication Sequence	Defines logon authentication method and precedence
RADIUS Client	Configures settings for authentication via a RADIUS server
TACACS+ Client	Configures settings for authentication via a TACACS+ server
AAA	Configures authentication, authorization, and accounting for network access
Web Server	Enables management access via a web browser
Telnet Server	Enables management access via Telnet
Secure Shell	Provides secure replacement for Telnet
802.1X Port Authentication	Configures host authentication on specific ports using 802.1X
Management IP Filter	Configures IP addresses that are allowed management access

3. For other methods of controlling client access, see [“General Security Measures” on page 259](#).

User Accounts and Privilege Levels

The basic commands required for management access and assigning command privilege levels are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection ([page 114](#)), user authentication via a remote authentication server ([page 199](#)), and host access authentication for specific ports ([page 244](#)).

Table 36: User Access Commands

Command	Function	Mode
enable password	Sets a password to control access to the Privileged Exec level	GC
username	Establishes a user name-based authentication system at login	GC
privilege	Assigns a privilege level to specified command groups or individual commands	GC
show privilege	Shows the privilege level for the current user, or the privilege level for commands modified by the privilege command	PE

enable password After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*

no enable password [**level** *level*]

level *level* - Sets the command access privileges. (Range: 0-15)

Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

Level 0-7 provide the same default access privileges, all within Normal Exec mode under the "Console>" command prompt.

Level 8-14 provide the same default access privileges, including additional commands in Normal Exec mode, and a subset of commands in Privileged Exec mode under the "Console#" command prompt.

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the [privilege](#) command.

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

password - Password for this privilege level.

(Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

The default is level 15.

The default password is "super"

Command Mode

Global Configuration

Command Usage

- ◆ You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the [enable](#) command.
- ◆ The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

[enable \(81\)](#)

[authentication enable \(204\)](#)

username This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

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

no username *name*

name - The name of the user. (Maximum length: 32 characters, case sensitive. Maximum users: 16)

The device has two predefined users, **guest** which is assigned privilege level **0** (Normal Exec) and has access to a limited number of commands, and **admin** which is assigned privilege level 15 and has full access to all commands.

access-level *level* - Specifies command access privileges. (Range: 0-15)

Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

Level 0-7 provide the same default access privileges, all within Normal Exec mode under the "Console>" command prompt.

Level 8-14 provide the same default access privileges, including additional commands in Normal Exec mode, and a subset of commands in Privileged Exec mode under the “Console#” command prompt.

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the [privilege](#) command.

Any privilege level can access all of the commands assigned to lower privilege levels. For example, privilege level 8 can access all commands assigned to privilege levels 7-0 according to default settings, and to any other commands assigned to levels 7-0 using the [privilege](#) command.

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

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

password *password* - The authentication password for the user. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

The default access level is 0 (Normal Exec).

The factory defaults for the user names and passwords are:

Table 37: Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup. There is no need for you to manually configure encrypted passwords.

Example

This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

privilege This command assigns a privilege level to specified command groups or individual commands. Use the **no** form to restore the default setting.

Syntax

privilege *mode* [**all**] **level** *level* *command*

no privilege *mode* [**all**] *command*

mode - The configuration mode containing the specified *command*.
(See [“Understanding Command Modes” on page 72](#) and [“Configuration Commands” on page 73](#).)

all - Modifies the privilege level for all subcommands under the specified *command*.

level *level* - Specifies the privilege level for the specified *command*. Refer to the default settings described for the access level parameter under the [username](#) command. (Range: 0-15)

command - Specifies any command contained within the specified *mode*.

Default Setting

Privilege level 0 provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Level 8 provides access to all display status and configuration commands, except for those controlling various authentication and security features. Level 15 provides full access to all commands.

Command Mode

Global Configuration

Example

This example sets the privilege level for the ping command to Privileged Exec.

```
Console(config)#privilege exec level 15 ping
Console(config)#
```

show privilege This command shows the privilege level for the current user, or the privilege level for commands modified by the [privilege](#) command.

Syntax

show privilege [**command**]

command - Displays the privilege level for all commands modified by the [privilege](#) command.

Command Mode

Privileged Exec

Example

This example shows the privilege level for any command modified by the [privilege](#) command.

```
Console#show privilege command
privilege line all level 0 accounting
privilege exec level 15 ping
Console(config)#
```

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 38: Authentication Sequence Commands

Command	Function	Mode
authentication enable	Defines the authentication method and precedence for command mode change	GC
authentication login	Defines logon authentication method and precedence	GC

authentication enable This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the [enable](#) command. Use the **no** form to restore the default.

Syntax

authentication enable {[local] [radius] [tacacs]}

no authentication enable

local - Use local password only.

radius - Use RADIUS server password only.

tacacs - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- ◆ RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

- ◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- ◆ You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication enable radius tacacs local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

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

Related Commands

enable password - sets the password for changing command modes (200)

authentication login This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[local] [radius] [tacacs]}

no authentication login

local - Use local password.

radius - Use RADIUS server password.

tacacs - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- ◆ RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- ◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

- ◆ You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication login radius tacacs local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

[username](#) - for setting the local user names and passwords (201)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 39: RADIUS Client Commands

Command	Function	Mode
radius-server acct-port	Sets the RADIUS server network port	GC
radius-server auth-port	Sets the RADIUS server network port	GC
radius-server host	Specifies the RADIUS server	GC
radius-server key	Sets the RADIUS encryption key sent in plain text	GC
radius-server encrypted-key	Sets the RADIUS encryption key sent in encrypted text	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC
show radius-server	Shows the current RADIUS settings	PE

radius-server acct-port This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

Syntax

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)

Default Setting

1813

Command Mode

Global Configuration

Example

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

**radius-server
auth-port** This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server auth-port *port-number*

no radius-server auth-port

port-number - RADIUS server UDP port used for authentication messages.
(Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

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

radius-server host This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

Syntax

[no] radius-server index host *host-ip-address* [**acct-port** *acct-port*] [**auth-port** *auth-port*] [**encrypted-key** *key*] [**retransmit** *retransmit*] [**key** *key*] [**retransmit** *retransmit*] [**timeout** *timeout*]

index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

host-ip-address - IP address of server.

acct-port - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)

auth-port - RADIUS server UDP port used for authentication messages.
(Range: 1-65535)

encrypted-key - Encryption key used to authenticate the Radius client with the server. Enclose ASCII characters limited to "A-Z" or "a-z". Note this key will be transmitted in encrypted text. (Maximum length: 48 characters)

key - Encryption key used to authenticate the Radius client with the server. Enclose any ASCII string (no blanks). Note this key will be transmitted in plain text. (Maximum length: 48 characters)

retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

auth-port - 1812

acct-port - 1813

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
retransmit 5 key green
Console(config)#
```

radius-server key This command sets the RADIUS encryption key to be sent in plain text. Use the **no** form to restore the default.

Syntax

radius-server key *key-string*

no radius-server key

key-string - Encryption key sent in plain text and used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes.
(Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server encrypted-key This command sets the RADIUS encryption key to be sent in encrypted text. Use the **no** form to restore the default.

Syntax

radius-server encrypted-key *key-string*

no radius-server key

key-string - Encryption key sent in encrypted text and used to authenticate logon access for client. Enclose any character string using ASCII characters "A-Z" or "a-z". (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server encrypted-key Z3JIZW4=
Console(config)#
```

radius-server retransmit This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
  Authentication Port Number : 1812
  Accounting Port Number    : 1813
  Retransmit Times          : 2
  Request Timeout           : 5

Server 1:
  Server IP Address         : 192.168.1.1
  Authentication Port Number : 1812
  Accounting Port Number    : 1813
  Retransmit Times          : 2
```

```

Request Timeout           : 5

RADIUS Server Group:
Group Name                Member Index
-----
radius                    1
Console#

```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 40: TACACS+ Client Commands

Command	Function	Mode
<code>tacacs-server host</code>	Specifies the TACACS+ server and optional parameters	GC
<code>tacacs-server key</code>	Sets the TACACS+ encryption key sent in plain text	GC
<code>tacacs-server encrypted-key</code>	Sets the TACACS+ encryption key sent in plain text	GC
<code>tacacs-server port</code>	Specifies the TACACS+ server network port	GC
<code>tacacs-server retransmit</code>	Sets the number of retries	GC
<code>tacacs-server timeout</code>	Sets the interval between sending authentication requests	GC
<code>show tacacs-server</code>	Shows the current TACACS+ settings	GC

tacacs-server host This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

Syntax

tacacs-server *index* **host** *host-ip-address* [**encrypted-key** *key*] [**key** *key*]
[**port** *port-number*] [**retransmit** *retransmit*] [**timeout** *timeout*]

no tacacs-server *index*

index - The index for this server. (Range: 1)

host-ip-address - IP address of a TACACS+ server.

encrypted-key - Encryption key used to authenticate the TACACS+ client with the server. Enclose ASCII characters limited to "A-Z" or "a-z". Note this key will be transmitted in encrypted text. (Maximum length: 48 characters)

key - Encryption key used to authenticate the TACACS+ client with the server. Enclose any ASCII string (no blanks). Note this key will be transmitted in plain text. (Maximum length: 48 characters)

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

retransmit - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Setting

authentication port - 49

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10
retransmit 5 key green
Console(config)#
```

tacacs-server key This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key-string*

no tacacs-server key

key-string - Encryption key sent in plain text and used to authenticate logon access for the client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

tacacs-server encrypted-key This command sets the TACACS+ encryption key to be sent in encrypted text. Use the **no** form to restore the default.

Syntax

radius-server encrypted-key *key-string*

no radius-server key

key-string - Encryption key sent in encrypted text and used to authenticate logon access for client. Enclose any character string using ASCII characters "A-Z" or "a-z". (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server encrypted-key Z3JIZW4=  
Console(config)#
```

tacacs-server port This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port-number*

no tacacs-server port

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181  
Console(config)#
```

tacacs-server retransmit This command sets the number of retries. Use the **no** form to restore the default.

Syntax

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

tacacs-server timeout This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

show tacacs-server This command displays the current settings for the TACACS+ server.

Default Setting
None

Command Mode
Privileged Exec

Example

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
  Server Port Number : 49
  Retransmit Times   : 2
  Timeout            : 5

Server 1:
  Server IP Address  : 10.11.12.13
  Server Port Number : 49
  Retransmit Times   : 2
  Timeout            : 4

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

AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

Table 41: AAA Commands

Command	Function	Mode
aaa accounting commands	Enables accounting of Exec mode commands	GC
aaa accounting dot1x	Enables accounting of 802.1X services	GC
aaa accounting exec	Enables accounting of Exec services	GC
aaa accounting update	Enables periodoc updates to be sent to the accounting server	GC
aaa authorization commands	Enables accounting of Exec mode commands	GC
aaa authorization exec	Enables authorization of Exec sessions	GC
aaa group server	Groups security servers in to defined lists	GC
server	Configures the IP address of a server in a group list	SG

Table 41: AAA Commands (Continued)

Command	Function	Mode
accounting dot1x	Applies an accounting method to an interface for 802.1X service requests	IC
accounting commands	Applies an accounting method to CLI commands entered by a user	Line
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	Line
authorization commands	Applies an authorization method to CLI commands entered by a user	Line
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	Line
show accounting	Displays all accounting information	PE
show authorization	Displays all authorization information	PE

aaa accounting commands This command enables the accounting of Exec mode commands. Use the **no** form to disable the accounting service.

Syntax

aaa accounting commands *level* {**default** | *method-name*} **start-stop** **group** {**tacacs+** | *server-group*}

no aaa accounting commands *level* {**default** | *method-name*}

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ The accounting of Exec mode commands is only supported by TACACS+ servers.
- ◆ Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

Example

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

aaa accounting dot1x This command enables the accounting of requested 802.1X services for network access. Use the **no** form to disable the accounting service.

Syntax

```
aaa accounting dot1x {default | method-name}
start-stop group {radius | tacacs+ | server-group}
no aaa accounting dot1x {default | method-name}
```

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the [radius-server host](#) command.

tacacs+ - Specifies all TACACS+ hosts configure with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

aaa accounting exec This command enables the accounting of requested Exec services for network access. Use the **no** form to disable the accounting service.

Syntax

```
aaa accounting exec {default | method-name}
start-stop group {radius | tacacs+ | server-group}
no aaa accounting exec {default | method-name}
```

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the [radius-server host](#) command.

tacacs+ - Specifies all TACACS+ hosts configure with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled

No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ This command runs accounting for Exec service requests for the local console and Telnet connections.
- ◆ Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update This command enables the sending of periodic updates to the accounting server. Use the **no** form to disable accounting updates.

Syntax

aaa accounting update [*periodic interval*]

no aaa accounting update

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

Default Setting

1 minute

Command Mode

Global Configuration

Command Usage

- ◆ When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.
- ◆ Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

Example

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization commands This command enables the authorization of Exec mode commands. Use the **no** form to disable the authorization service.

Syntax

aaa authorization commands *level* {**default** | *method-name*} **start-stop** **group** {**tacacs+** | *server-group*}

no aaa authorization commands *level* {**default** | *method-name*}

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default authorization method for service requests.

method-name - Specifies an authorization method for service requests.
(Range: 1-64 characters)

start-stop - Records authorization from starting point and stopping point.

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Authorization is not enabled

No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ The authorization of Exec mode commands is only supported by TACACS+ servers.
- ◆ Note that the **default** and *method-name* fields are only used to describe the authorization method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

Example

```
Console(config)#aaa authorization commands 15 default start-stop group  
tacacs+  
Console(config)#
```

aaa authorization exec This command enables the authorization for Exec access. Use the **no** form to disable the authorization service.

Syntax

aaa authorization exec {**default** | *method-name*}
group {**tacacs+** | *server-group*}

no aaa authorization exec {**default** | *method-name*}

default - Specifies the default authorization method for Exec access.

method-name - Specifies an authorization method for Exec access.
(Range: 1-64 characters)

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Authorization is not enabled

No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ This command performs authorization to determine if a user is allowed to run an Exec shell for local console, Telnet, or SSH connections.
- ◆ AAA authentication must be enabled before authorization is enabled.
- ◆ If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

Example

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

aaa group server Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the **no** form of this command.

Syntax

[no] aaa group server {radius | tacacs+} group-name

radius - Defines a RADIUS server group.

tacacs+ - Defines a TACACS+ server group.

group-name - A text string that names a security server group.
(Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server This command adds a security server to an AAA server group. Use the **no** form to remove the associated server from the group.

Syntax

[no] server {*index* | *ip-address*}

index - Specifies the server index. (Range: RADIUS 1-5, TACACS+ 1)

ip-address - Specifies the host IP address of a server.

Default Setting

None

Command Mode

Server Group Configuration

Command Usage

- ◆ When specifying the index for a RADIUS server, that server index must already be defined by the [radius-server host](#) command.
- ◆ When specifying the index for a TACACS+ server, that server index must already be defined by the [tacacs-server host](#) command.

Example

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x This command applies an accounting method for 802.1X service requests on an interface. Use the **no** form to disable accounting on the interface.

Syntax

accounting dot1x {**default** | *list-name*}

no accounting dot1x

default - Specifies the default method list created with the [aaa accounting dot1x](#) command.

list-name - Specifies a method list created with the [aaa accounting dot1x](#) command.

Default Setting

None

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting commands This command applies an accounting method to entered CLI commands. Use the **no** form to disable accounting for entered CLI commands.

Syntax

accounting commands *level* {**default** | *list-name*}

no accounting commands *level*

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default method list created with the [aaa accounting commands](#) command.

list-name - Specifies a method list created with the [aaa accounting commands](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#accounting commands 15 default
Console(config-line)#
```

accounting exec This command applies an accounting method to local console, Telnet or SSH connections. Use the **no** form to disable accounting on the line.

Syntax

accounting exec {**default** | *list-name*}

no accounting exec

default - Specifies the default method list created with the [aaa accounting exec](#) command.

list-name - Specifies a method list created with the [aaa accounting exec](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

authorization commands This command applies an authorization method to entered CLI commands. Use the **no** form to disable authorization for entered CLI commands.

Syntax

authorization commands *level* {**default** | *list-name*}

no authorization commands *level*

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default method list created with the [aaa authorization commands](#) command.

list-name - Specifies a method list created with the [aaa authorization commands](#) command.

Default Setting

None

Command Mode

Line Configuration

Command Usage

If for example the command “authorization commands 0” is executed, the switch will block all commands issued by a privileged level 0 user. Approved commands for the user level must be configured on the AAA server.

Example

```
Console(config)#line console
Console(config-line)#authorization commands 15 default
Console(config-line)#
```


authorization exec This command applies an authorization method to local console, Telnet or SSH connections. Use the **no** form to disable authorization on the line.

Syntax

authorization exec {**default** | *list-name*}

no authorization exec

default - Specifies the default method list created with the **aaa authorization exec** command.

list-name - Specifies a method list created with the **aaa authorization exec** command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

show accounting This command displays the current accounting settings per function and per port.

Syntax

show accounting [**commands** [*level*]] |
[[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] |
exec [**statistics**] | **statistics**]

commands - Displays command accounting information.

level - Displays command accounting information for a specifiable command level.

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     : Eth 1/1

  Method List   : tps
  Group List    : radius
  Interface     : Eth 1/2

Accounting Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Accounting Type : Commands 0
  Method List   : default
  Group List    : tacacs+
  Interface     :
:
Accounting Type : Commands 15
  Method List   : default
  Group List    : tacacs+
  Interface     :

Console#

```

show authorization This command displays the current authorization settings per function and per port.

Syntax

show authorization [**commands** [*level*] | **exec**]

commands - Displays command authorization information.

level - Displays command authorization information for a specifiable command level.

exec - Displays Exec authorization records.

Default Setting
None

Command Mode
Privileged Exec

Example

```
Console#show authorization
Authorization Type : EXEC
  Method List      : default
  Group List       : tacacs+
  Interface        : vty

Authorization Type : Commands 0
  Method List      : default
  Group List       : tacacs+
  Interface        :
:
Authorization Type : Commands 15
  Method List      : default
  Group List       : tacacs+
  Interface        :

Console#
```

Web Server

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

Table 42: Web Server Commands

Command	Function	Mode
ip http authentication	Sets the method list for EXEC authorization of an EXEC session	GC
ip http port	Specifies the port to be used by the web browser interface	GC
ip http server	Allows the switch to be monitored or configured from a browser	GC
ip http secure-port	Specifies the TCP port number for HTTPS	GC
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC
show authorization	Displays all authorization information	PE
show system	Displays system information	NE, PE



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

ip http authentication This command specifies the method list for EXEC authorization for starting an EXEC session used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http authentication aaa exec-authorization {default | *list-name*}

no ip http authentication aaa exec-authorization

default - Specifies the default method list used for authorization requests.

list-name - Specifies a method list created with the [aaa authorization commands](#) command.

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip http authentication aaa exec-authorization default
Console(config)#
```

Related Commands

[aaa authorization commands \(219\)](#)

[ip http server \(229\)](#)

[show system \(95\)](#)

ip http port This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*

no ip http port

port-number - The TCP port to be used by the browser interface.
(Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769  
Console(config)#
```

Related Commands

[ip http server \(229\)](#)

[show system \(95\)](#)

ip http server This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[no] ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server  
Console(config)#
```

Related Commands

[ip http authentication \(228\)](#)

[show system \(95\)](#)

ip http secure-port This command specifies the TCP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*

no ip http secure-port

port_number – The TCP port used for HTTPS. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- ◆ You cannot configure the HTTP and HTTPS servers to use the same port.
- ◆ If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://device:port_number**

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

[ip http secure-server \(230\)](#)
[show system \(95\)](#)

ip http secure-server This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[no] ip http secure-server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- ◆ If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https://device[:port_number]**
- ◆ When you start HTTPS, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.

- ◆ The client and server establish a secure encrypted connection.

A padlock icon should appear in the status bar for Internet Explorer 11, Mozilla Firefox 40, or Google Chrome 45, or more recent versions.

The following web browsers and operating systems currently support HTTPS:

Table 43: HTTPS System Support

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

- ◆ To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” in the *Web Management Guide*. Also refer to the [copy tftp https-certificate](#) command.
- ◆ Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

[ip http secure-port \(229\)](#)
[copy tftp https-certificate \(103\)](#)
[show system \(95\)](#)

Telnet Server

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

Table 44: Telnet Server Commands

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



Note: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

ip telnet max-sessions This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** form to restore the default setting.

Syntax

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count - The maximum number of allowed Telnet session.
(Range: 0-8)

Default Setting

8 sessions

Command Mode

Global Configuration

Command Usage

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

Example

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

ip telnet port This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

Syntax

ip telnet port *port-number*

no telnet port

port-number - The TCP port number to be used by the browser interface.
(Range: 1-65535)

Default Setting

23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet port 123  
Console(config)#
```

ip telnet server This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

Syntax

[no] ip telnet server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server  
Console(config)#
```

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

Syntax

telnet *host*

host - IP address or alias of a remote device.

Command Mode

Privileged Exec

Example

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

show ip telnet This command displays the configuration settings for the Telnet server.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 8
Console#
```

Secure Shell

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.



Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 45: Secure Shell Commands

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

Table 45: Secure Shell Commands (Continued)

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

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the `authentication login` command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the `ip ssh crypto host-key generate` command to create a host public/private key pair.
2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

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

3. Import Client's Public Key to the Switch – Use the `copy tftp public-key` command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the `username` command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

```
1024 35
134108168560989392104094492015542534763164192187295892114317388005553616163105
177594083868631109291232226828519254374603100937187721199696317813662774141689
851320491172048303392543241016379975923714490119380060902539484084827178194372
288402533115952134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. Enable SSH Service – Use the `ip ssh server` command to enable the SSH server on the switch.
6. *Authentication* – One of the following authentication methods is employed:

Password Authentication (for SSH v1.5 or V2 Clients)

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



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

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

- a. The client sends its RSA public key to the switch.
- b. The switch compares the client's public key to those stored in memory.
- c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.
- d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
- e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

- a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
- b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
- c. The client sends a signature generated using the private key to the switch.

- d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.



Note: The SSH server supports up to eight client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Note: The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

ip ssh authentication-retries This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

Related Commands

[show ip ssh \(242\)](#)

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

Syntax

[no] ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The SSH server supports up to eight client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- ◆ The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- ◆ You must generate DSA and RSA host keys before enabling the SSH server.

Example

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

Related Commands

[ip ssh crypto host-key generate \(240\)](#)

[show ssh \(243\)](#)

ip ssh server-key size This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

The server key is a private key that is never shared outside the switch. The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

ip ssh timeout This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation.
(Range: 1-120)

Default Setting

120 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the [exec-timeout](#) command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

[exec-timeout \(116\)](#)

[show ip ssh \(242\)](#)

delete public-key This command deletes the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

username – Name of an SSH user. (Range: 1-32 characters)

dsa – DSA public key type.

rsa – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [dsa | rsa]

dsa – DSA (Version 2) key type.

rsa – RSA (Version 1) key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- ◆ The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- ◆ This command stores the host key pair in memory (i.e., RAM). Use the [ip ssh save host-key](#) command to save the host key pair to flash memory.
- ◆ Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- ◆ The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

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

Related Commands

[ip ssh crypto zeroize \(241\)](#)

[ip ssh save host-key \(241\)](#)

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

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

dsa – DSA key type.

rsa – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- ◆ This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- ◆ The SSH server must be disabled before you can execute this command.

Example

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

Related Commands

[ip ssh crypto host-key generate \(240\)](#)

[ip ssh save host-key \(241\)](#)

[no ip ssh server \(237\)](#)

ip ssh save host-key This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key
Console#
```

Related Commands

[ip ssh crypto host-key generate \(240\)](#)

show ip ssh This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size      : 768 bits
Console#
```

show public-key This command shows the public key for the specified user or for the host.

Syntax

show public-key [user [username]] host]

username – Name of an SSH user. (Range: 1-32 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- ◆ If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- ◆ When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
071942106165575942459093923609695405036277525755625100386613098939383452310
332802149888661921595568598879891919505883940181387440468908779160305837768
```

```
185490002831341625008348718449522087429212255691665655296328163516964040831
5547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFFAKx15fwFfv
JlPdOkFgzLGMInvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMacNBpJBrRAAAAFQChb4vvsdfQGNIjwbv
wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOFT/yyEfbbobMJZi8oGCstSN0xrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq70+jAhf1Dg45loAc27s6TLdtnylwRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bs2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#
```

show ssh This command displays the current SSH server connections.

Command Mode
Privileged Exec

Example

```
Console#show ssh
Connection Version State Username Encryption
1 2.0 Session-Started admin ctos aes128-cbc-hmac-md5
stoc aes128-cbc-hmac-md5
Console#
```

Table 46: show ssh - display description

Field	Description
Connection	The session number. (Range: 1-8)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 47: 802.1X Port Authentication Commands

Command	Function	Mode
<i>General Commands</i>		
<code>dot1x default</code>	Resets all dot1x parameters to their default values	GC
<code>dot1x system-auth-control</code>	Enables dot1x globally on the switch.	GC
<i>Authenticator Commands</i>		
<code>dot1x intrusion-action</code>	Sets the port response to intrusion when authentication fails	IC
<code>dot1x max-reauth-req</code>	Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process	IC
<code>dot1x max-req</code>	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC
<code>dot1x operation-mode</code>	Allows single or multiple hosts on an dot1x port	IC
<code>dot1x port-control</code>	Sets dot1x mode for a port interface	IC
<code>dot1x re-authentication</code>	Enables re-authentication for all ports	IC
<code>dot1x timeout quiet-period</code>	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC
<code>dot1x timeout re-authperiod</code>	Sets the time period after which a connected client must be re-authenticated	IC
<code>dot1x timeout supp-timeout</code>	Sets the interval for a supplicant to respond	IC
<code>dot1x timeout tx-period</code>	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC
<code>dot1x re-authenticate</code>	Forces re-authentication on specific ports	PE
<i>Information Display Commands</i>		
<code>show dot1x</code>	Shows all dot1x related information	PE

General Commands

dot1x default This command sets all configurable dot1x authenticator global and port settings to their default values.

Command Mode
Global Configuration

Command Usage

This command resets the following commands to their default settings:

- ◆ dot1x system-auth-control
- ◆ dot1x eapol-pass-through
- ◆ dot1x port-control
- ◆ dot1x port-control multi-host max-count
- ◆ dot1x operation-mode
- ◆ dot1x max-req
- ◆ dot1x timeout quiet-period
- ◆ dot1x timeout tx-period
- ◆ dot1x timeout re-authperiod
- ◆ dot1x timeout sup-timeout
- ◆ dot1x re-authentication
- ◆ dot1x intrusion-action

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x system-auth-control This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[no] dot1x system-auth-control

Default Setting

Disabled

Command Mode

Global Configuration

Example

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

Authenticator Commands

dot1x intrusion-action This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the **no** form to reset the default.

Syntax

dot1x intrusion-action {block-traffic | guest-vlan}

no dot1x intrusion-action

block-traffic - Blocks traffic on this port.

guest-vlan - Assigns the user to the Guest VLAN.

Default

block-traffic

Command Mode

Interface Configuration

Command Usage

- ◆ For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the [vlan database](#) command) and assigned as the guest VLAN for the port (see the [network-access guest-vlan](#) command).
- ◆ A port can only be assigned to the guest VLAN in case of failed authentication, if [switchport mode](#) is set to Hybrid.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

dot1x max-reauth-req This command sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. Use the **no** form to restore the default.

Syntax

dot1x max-reauth-req *count*

no dot1x max-reauth-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-reauth-req 2
Console(config-if)#
```

dot1x max-req This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x operation-mode This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

single-host – Allows only a single host to connect to this port.

multi-host – Allows multiple host to connect to this port.

max-count – Keyword for the maximum number of hosts.

count – The maximum number of hosts that can connect to a port.
(Range: 1-1024; Default: 5)

mac-based – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- ◆ The “max-count” parameter specified by this command is only effective if the dot1x mode is set to “auto” by the [dot1x port-control](#) command.
- ◆ In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- ◆ In “mac-based-auth” mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```


dot1x port-control This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

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

no dot1x port-control

auto – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

force-authorized – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

force-unauthorized – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authentication This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

[no] dot1x re-authentication

Command Mode

Interface Configuration

Command Usage

- ◆ The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- ◆ The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.

Example

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

Related Commands

[dot1x timeout re-authperiod \(250\)](#)

dot1x timeout quiet-period This command sets the time that a switch port waits after the maximum request count (see [page 247](#)) has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout supp-timeout This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Command Usage

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

dot1x timeout tx-period This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default
30 seconds

Command Mode
Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

dot1x re-authenticate This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode
Privileged Exec

Command Usage

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

Example

```
Console#dot1x re-authenticate
Console#
```

Information Display Commands

show dot1x This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- ◆ *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch ([page 245](#)).
- ◆ *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
 - Type – Administrative state for port access control (Enabled, Authenticator, or Supplicant).
 - Operation Mode – Allows single or multiple hosts ([page 248](#)).
 - Control Mode – Dot1x port control mode ([page 249](#)).
 - Authorized – Authorization status (yes or n/a - not authorized).
- ◆ *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
 - Reauthentication – Periodic re-authentication ([page 249](#)).
 - Reauth Period – Time after which a connected client must be re-authenticated ([page 250](#)).
 - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client ([page 250](#)).
 - TX Period – Time a port waits during authentication session before re-transmitting EAP packet ([page 251](#)).
 - Supplicant Timeout – Supplicant timeout.
 - Server Timeout – Server timeout. A RADIUS server must be set before the correct operational value of 10 seconds will be displayed in this field.
 - Reauth Max Retries – Maximum number of reauthentication attempts.
 - Max Request – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session ([page 247](#)).

- Operation Mode– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
- Port Control–Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized ([page 249](#)).
- Intrusion Action– Shows the port response to intrusion when authentication fails ([page 246](#)).
- Supplicant– MAC address of authorized client.

◆ *Authenticator PAE State Machine*

- State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- Reauth Count– Number of times connecting state is re-entered.
- Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

◆ *Backend State Machine*

- State – Current state (including request, response, success, fail, timeout, idle, initialize).
- Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
- Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

◆ *Reauthentication State Machine*

State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
  System Auth Control      : Enabled

Authenticator Parameters:
  EAPOL Pass Through      : Disabled

802.1X Port Summary

Port      Type      Operation Mode Control Mode      Authorized
-----
Eth 1/ 1 Disabled    Single-Host      Force-Authorized   Yes
Eth 1/ 2 Disabled    Single-Host      Force-Authorized   Yes
'''
Eth 1/25 Disabled    Single-Host      Force-Authorized   Yes
Eth 1/26 Enabled      Single-Host      Auto                Yes

Console#show dot1x interface ethernet 1/2

802.1X Authenticator is enabled on port 2
Reauthentication      : Enabled
Reauth Period         : 3600
Quiet Period          : 60
TX Period              : 30
Supplicant Timeout    : 30
Server Timeout        : 10
```

```

Reauth Max Retries      : 2
Max Request             : 2
Operation Mode          : Multi-host
Port Control            : Auto
Intrusion Action        : Block traffic

Supplicant               : 00-e0-29-94-34-65

Authenticator PAE State Machine
State                   : Authenticated
Reauth Count            : 0
Current Identifier      : 3

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

Reauthentication State Machine
State                   : Initialize
Console#

```

Management IP Filter

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

Table 48: Management IP Filter Commands

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

management This command specifies the client IP addresses that are allowed management access to the switch through various protocols. A list of up to 15 IP addresses or IP address groups can be specified. Use the **no** form to restore the default setting.

Syntax

[no] management {all-client | http-client | snmp-client | telnet-client}
start-address [end-address]

all-client - Adds IP address(es) to all groups.

http-client - Adds IP address(es) to the web group.

snmp-client - Adds IP address(es) to the SNMP group.

telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

end-address - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- ◆ The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- ◆ If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- ◆ IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- ◆ When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- ◆ You cannot delete an individual address from a specified range. You must delete the entire range, and re-enter the addresses.
- ◆ You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {all-client | http-client | snmp-client | telnet-client}

all-client - Displays IP addresses for all groups.

http-client - Displays IP addresses for the web group.

snmp-client - Displays IP addresses for the SNMP group.

telnet-client - Displays IP addresses for the Telnet group.

Command Mode
Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
  HTTP-Client:
    Start IP address      End IP address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

  SNMP-Client:
    Start IP address      End IP address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

  TELNET-Client:
    Start IP address      End IP address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

Console#
```


General Security Measures

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Port-based authentication using IEEE 802.1X is commonly used for these purposes. In addition to these method, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

Table 49: General Security Commands

Command Group	Function
Port Security*	Configures secure addresses for a port
802.1X Port Authentication*	Configures host authentication on specific ports using 802.1X
Network Access*	Configures MAC authentication and dynamic VLAN assignment
Web Authentication*	Configures Web authentication
Access Control Lists*	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
DHCPv4 Snooping*	Filters untrusted DHCPv4 messages on unsecure ports by building and maintaining a DHCPv4 snooping binding table
IPv4 Source Guard*	Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets
DoS Protection	Protects against Denial-of-Service attacks
Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, DHCP Snooping, and then IPv4 Source Guard.

Port Security

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 50: Management IP Filter Commands

Command	Function	Mode
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>mac-learning</code>	Enables MAC address learning on the selected physical interface or VLAN	IC
<code>port security</code>	Configures a secure port	IC
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show port security</code>	Displays port security status and secure address count	PE

mac-learning This command enables MAC address learning on the selected interface. Use the **no** form to disable MAC address learning.

Syntax

[no] mac-learning

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet or Port Channel)

Command Usage

- ◆ The **no mac-learning** command immediately stops the switch from learning new MAC addresses on the specified port or trunk. Incoming traffic with source addresses not stored in the static address table, will be flooded. However, if a security function such as 802.1X or DHCP snooping is enabled and mac-learning is disabled, then only incoming traffic with source addresses stored in

the static address table will be accepted, all other packets are dropped. Note that the dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled.

- ◆ The mac-learning commands cannot be used if 802.1X Port Authentication has been globally enabled on the switch with the [dot1x system-auth-control](#) command, or if MAC Address Security has been enabled by the [port security](#) command on the same interface.

Example

The following example disables MAC address learning for port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

Related Commands

[show interfaces status \(364\)](#)

port security This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable port.

max-mac-count

address-count - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

Status: Disabled

Action: None

Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The default maximum number of MAC addresses allowed on a secure port is zero (that is, port security is disabled). To use port security, you must configure the maximum number of addresses allowed on a port using the **port security max-mac-count** command.
- ◆ When port security is enabled using the **port security** command, or the maximum number or allowed addresses is set to a value lower than the current limit after port security has been enabled, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- ◆ To configure the maximum number of address entries which can be learned on a port, specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. (The specified maximum address count is effective when port security is enabled or disabled.) Note that you can manually add additional secure addresses to a port using the **mac-address-table static** command. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.
- ◆ If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.
- ◆ If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.
- ◆ A secure port has the following restrictions:
 - Cannot be connected to a network interconnection device.
 - Cannot be a trunk port.
 - RSPAN and port security are mutually exclusive functions. If port security is enabled on a port, that port cannot be set as an RSPAN uplink port. Also, when a port is configured as an RSPAN uplink port, source port, or destination port, port security cannot be enabled on that port.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands[show interfaces status \(364\)](#)[shutdown \(356\)](#)[mac-address-table static \(426\)](#)**show port security** This command displays port security status and the secure address count.**Syntax****show port security** [**interface** *interface*]*interface* - Specifies a port interface.**ethernet** *unit/port**unit* - Unit identifier. (Range: 1)*port* - Port number. (Range: 1-10/28)**Command Mode**

Privileged Exec

Example

This example shows the port security settings and number of secure addresses for all ports.

```

Console#show port security
Global Port Security Parameters
Secure MAC Aging Mode : Disabled

Port Security Port Summary
Port      Port Security Port Status  Intrusion Action  MaxMacCnt  CurrMacCnt
-----
Eth 1/ 1 Disabled      Secure/Down  None          0          2
Eth 1/ 2 Enabled      Secure/Up    None         10          0
Eth 1/ 3 Disabled      Secure/Down  None          0          0
Eth 1/ 4 Disabled      Secure/Down  None          0          0
Eth 1/ 5 Disabled      Secure/Down  None          0          0
.
.
.

```

Table 51: show port security - display description

Field	Description
Port Security	The configured status (enabled or disabled).
Port Status	The operational status: <ul style="list-style-type: none"> ◆ Secure/Down – Port security is disabled. ◆ Secure/Up – Port security is enabled. ◆ Shutdown – Port is shut down due to a response to a port security violation.
Intrusion Action	The configured intrusion response.

Table 51: show port security - display description (Continued)

Field	Description
MaxMacCnt	The maximum number of addresses which can be stored in the address table for this interface (either dynamic or static).
CurrMacCnt	The current number of secure entries in the address table.

The following example shows the port security settings and number of secure addresses for a specific port. The Last Intrusion MAC and Last Time Detected Intrusion MAC fields show information about the last detected intrusion MAC address. These fields are not applicable if no intrusion has been detected or port security is disabled. The MAC Filter ID field is configured by the [network-access mac-filter](#) command. If this field displays Disabled, then any unknown source MAC address can be learned as a secure MAC address. If it displays a filter identifier, then only source MAC address entries in MAC Filter table can be learned as secure MAC addresses.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC Aging Mode : Disabled

Port Security Details
Port                               : 1/2
Port Security                     : Enabled
Port Status                       : Secure/Up
Intrusion Action                   : None
Max MAC Count                     : 0
Current MAC Count                 : 0
MAC Filter                        : Disabled
Last Intrusion MAC                : NA
Last Time Detected Intrusion MAC  : NA
Console#
```

This example shows information about a detected intrusion.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC Aging Mode : Disabled

Port Security Details
Port                               : 1/2
Port Security                     : Enabled
Port Status                       : Secure/Up
Intrusion Action                   : None
Max MAC Count                     : 0
Current MAC Count                 : 0
MAC Filter                        : Disabled
Last Intrusion MAC                : 00-10-22-00-00-01
Last Time Detected Intrusion MAC  : 2015/7/29 15:13:03
Console#
```


Network Access (MAC Address Authentication)

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

Table 52: Network Access Commands

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

network-access aging Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the **no** form of this command to disable address aging.

Syntax

[no] network-access aging

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the [mac-address-table aging-time](#) command.
- ◆ This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on [page 248](#)).
- ◆ The maximum number of secure MAC addresses supported for the switch system is 1024.

Example

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

network-access mac-filter Use this command to add a MAC address into a filter table. Use the **no** form of this command to remove the specified MAC address.

Syntax

[no] network-access mac-filter *filter-id*
mac-address *mac-address* [**mask** *mask-address*]

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

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for a range of addresses.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Specified addresses are exempt from network access authentication.

- ◆ This command is different from configuring static addresses with the `mac-address-table static` command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the `network-access mac-filter` command.
- ◆ Up to 64 filter tables can be defined.
- ◆ There is no limitation on the number of entries that can entered in a filter table.

Example

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66  
Console(config)#
```

mac-authentication reauth-time Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the **no** form of this command to restore the default value.

Syntax

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

seconds - The reauthentication time period. (Range: 120-1000000 seconds)

Default Setting

1800

Command Mode

Global Configuration

Command Usage

- ◆ The reauthentication time is a global setting and applies to all ports.
- ◆ When the reauthentication time expires for a secure MAC address it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected.

Example

```
Console(config)#mac-authentication reauth-time 300  
Console(config)#
```

network-access Use this command to enable the dynamic QoS feature for an authenticated port.
dynamic-qos Use the **no** form to restore the default.

Syntax

[no] network-access dynamic-qos

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The “Filter-ID” attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 53: Dynamic QoS Profiles

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

- ◆ When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- ◆ When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- ◆ While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.



Note: Any configuration changes for dynamic QoS are not saved to the switch configuration file.

Example

The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

Syntax

[no] network-access dynamic-vlan

Default Setting

Enabled

Command Mode

Interface Configuration

Command Usage

- ◆ When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch.
- ◆ The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- ◆ If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- ◆ When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

Example

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication or MAC authentication is rejected. Use the **no** form of this command to disable guest VLAN assignment.

Syntax

network-access guest-vlan *vlan-id*

no network-access guest-vlan

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ The VLAN to be used as the guest VLAN must be defined and set as active (See the [vlan database](#) command).
- ◆ When used with 802.1X authentication, the intrusion-action must be set for "guest-vlan" to be effective (see the [dot1x intrusion-action](#) command).
- ◆ A port can only be assigned to the guest VLAN in case of failed authentication, if [switchport mode](#) is set to Hybrid.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access max-mac-count Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the **no** form of this command to restore the default.

Syntax

network-access max-mac-count *count*

no network-access max-mac-count

count - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 0-1024; 0 for unlimited)

Default Setting

1024

Command Mode

Interface Configuration

Command Usage

The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

Example

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

network-access mode mac-authentication Use this command to enable network access authentication on a port. Use the **no** form of this command to disable network access authentication.

Syntax

[no] network-access mode mac-authentication

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.
- ◆ On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).
- ◆ Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.
- ◆ Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- ◆ MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.
- ◆ MAC authentication cannot be configured on trunks (i.e., static nor dynamic).

- ◆ When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- ◆ The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t," where "u" indicates untagged VLAN and "t" tagged VLAN. The "Tunnel-Type" attribute should be set to "VLAN," and the "Tunnel-Medium-Type" attribute set to "802."

Example

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

network-access port-mac-filter Use this command to enable the specified MAC address filter. Use the **no** form of this command to disable the specified MAC address filter.

Syntax

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

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

Default Setting

None

Command Mode

Interface Configuration

Command Mode

- ◆ Entries in the MAC address filter table can be configured with the [network-access mac-filter](#) command.
- ◆ Only one filter table can be assigned to a port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```


mac-authentication intrusion-action Use this command to configure the port response to a host MAC authentication failure. Use the **no** form of this command to restore the default.

Syntax

mac-authentication intrusion-action {block traffic | pass traffic}
no mac-authentication intrusion-action

Default Setting

Block Traffic

Command Mode

Interface Configuration

Example

```
Console(config-if)#mac-authentication intrusion-action block-traffic  
Console(config-if)#
```

mac-authentication max-mac-count Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the **no** form of this command to restore the default.

Syntax

mac-authentication max-mac-count *count*
no mac-authentication max-mac-count

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

Default Setting

1024

Command Mode

Interface Configuration

Example

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

clear network-access Use this command to clear entries from the secure MAC addresses table.

Syntax

clear network-access mac-address-table [**static** | **dynamic**]
[**address** *mac-address*] [**interface** *interface*]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

show network-access Use this command to display the MAC authentication settings for port interfaces.

Syntax

show network-access [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Default Setting

Displays the settings for all interfaces.

Command Mode

Privileged Exec

Example

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time                : 1800
MAC Address Aging                   : Disabled

Port : 1/1
MAC Authentication                   : Disabled
MAC Authentication Intrusion Action : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts                  : 1024
Dynamic VLAN Assignment              : Enabled
Dynamic QoS Assignment               : Disabled
MAC Filter ID                       : Disabled
Guest VLAN                          : Disabled
Console#
```

show network-access mac-address-table Use this command to display secure MAC address table entries.

Syntax

show network-access mac-address-table [**static** | **dynamic**]
[**address** *mac-address* [*mask*]] [**interface** *interface*] [**sort** {**address** |
interface}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

sort - Sorts displayed entries by either MAC address or interface.

Default Setting

Displays all filters.

Command Mode

Privileged Exec

Command Usage

When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don't care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-00-00-00 would result in all MACs in the range 00-00-01-00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

Example

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

Console#
```

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

Syntax

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

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

Default Setting

Displays all filters.

Command Mode

Privileged Exec

Example

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

Console#
```

Web Authentication

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.



Note: RADIUS authentication must be activated and configured for the web authentication feature to work properly (see [“Authentication Sequence” on page 204](#)).

Note: Web authentication cannot be configured on trunk ports.

Table 54: Web Authentication

Command	Function	Mode
<code>web-auth login-attempts</code>	Defines the limit for failed web authentication login attempts	GC
<code>web-auth quiet-period</code>	Defines the amount of time to wait after the limit for failed login attempts is exceeded.	GC
<code>web-auth session-timeout</code>	Defines the amount of time a session remains valid	GC
<code>web-auth system-auth-control</code>	Enables web authentication globally for the switch	GC
<code>web-auth</code>	Enables web authentication for an interface	IC
<code>web-auth re-authenticate (Port)</code>	Ends all web authentication sessions on the port and forces the users to re-authenticate	PE
<code>web-auth re-authenticate (IP)</code>	Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate	PE
<code>show web-auth</code>	Displays global web authentication parameters	PE
<code>show web-auth interface</code>	Displays interface-specific web authentication parameters and statistics	PE
<code>show web-auth summary</code>	Displays a summary of web authentication port parameters and statistics	PE

web-auth login-attempts This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the **no** form to restore the default.

Syntax

web-auth login-attempts *count*

no web-auth login-attempts

count - The limit of allowed failed login attempts. (Range: 1-3)

Default Setting

3 login attempts

Command Mode

Global Configuration

Example

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

web-auth quiet-period This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

Syntax

web-auth quiet-period *time*

no web-auth quiet period

time - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

Default Setting

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth session-timeout This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

Syntax

web-auth session-timeout *timeout*

no web-auth session timeout

timeout - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

Default Setting

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

web-auth system-auth-control This command globally enables web authentication for the switch. Use the **no** form to restore the default.

Syntax

[no] web-auth system-auth-control

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Both **web-auth system-auth-control** for the switch and **web-auth** for an interface must be enabled for the web authentication feature to be active.

Example

```
Console(config)#web-auth system-auth-control
Console(config)#
```

web-auth This command enables web authentication for an interface. Use the **no** form to restore the default.

Syntax

[no] web-auth

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

Both **web-auth system-auth-control** for the switch and **web-auth** for a port must be enabled for the web authentication feature to be active.

Example

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

web-auth re-authenticate (Port) This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

Syntax

web-auth re-authenticate interface *interface*

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#web-auth re-authenticate interface ethernet 1/2
Console#
```

web-auth re-authenticate (IP) This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

Syntax

web-auth re-authenticate interface *interface ip*

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

ip - IPv4 formatted IP address

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```


show web-auth This command displays global web authentication parameters.

Command Mode

Privileged Exec

Example

```
Console#show web-auth
Global Web-Auth Parameters
  System Auth Control      : Enabled
  Session Timeout          : 3600
  Quiet Period             : 60
  Max Login Attempts       : 3
Console#
```

show web-auth interface This command displays interface-specific web authentication parameters and statistics.

Syntax

show web-auth interface *interface*

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

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

Host Summary

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

show web-auth summary This command displays a summary of web authentication port parameters and statistics.

Command Mode
Privileged Exec

Example

```
Console#show web-auth summary
Global Web-Auth Parameters
  System Auth Control      : Enabled
Port      Status          Authenticated Host Count
----      -
1/ 1      Disabled        0
1/ 2      Enabled         8
1/ 3      Disabled        0
1/ 4      Disabled        0
1/ 5      Disabled        0
:
```

DHCPv4 Snooping

DHCPv4 snooping allows a switch to protect a network from rogue DHCPv4 servers or other devices which send port-related information to a DHCPv4 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv4 snooping.

Table 55: DHCP Snooping Commands

Command	Function	Mode
ip dhcp snooping	Enables DHCP snooping globally	GC
ip dhcp snooping information option	Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id	GC
ip dhcp snooping information option encode no-subtype	Disables use of sub-type and sub-length for the CID/RID in Option 82 information	GC
ip dhcp snooping information option remote-id	Sets the remote ID to the switch's IP address, MAC address, or arbitrary string, TR-101 compliant node identifier, or removes VLAN ID from the end of the TR101 field	GC
ip dhcp snooping information option tr101 board-id	Sets the board identifier used in Option 82 information based on TR-101 syntax	GC
ip dhcp snooping information policy	Sets the information option policy for DHCP client packets that include Option 82 information	GC
ip dhcp snooping verify mac-address	Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLAN	GC
ip dhcp snooping information option circuit-id	Enables or disables the use of DHCP Option 82 information circuit-id suboption	IC

Table 55: DHCP Snooping Commands (Continued)

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

ip dhcp snooping This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the `ip dhcp snooping vlan` command, DHCP messages received on an untrusted interface (as specified by the `no ip dhcp snooping trust` command) from a device not listed in the DHCP snooping table will be dropped.
- ◆ When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- ◆ Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- ◆ When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.
- ◆ Filtering rules are implemented as follows:
 - If global DHCP snooping is disabled, all DHCP packets are forwarded.
 - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
 - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
 - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
 - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
 - If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the `ip dhcp snooping verify mac-address` command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
 - If the DHCP packet is not a recognizable type, it is dropped.
 - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
 - If a DHCP packet from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- ◆ If DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
- ◆ *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the `ip dhcp snooping trust` command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the

switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Example

This example enables DHCP snooping globally for the switch.

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

Related Commands

[ip dhcp snooping vlan \(291\)](#)

[ip dhcp snooping trust \(294\)](#)

ip dhcp snooping information option

This command enables the use of DHCP Option 82 information for the switch, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the **no** form without any keywords to disable this function.



Note: Further optional details can be found in the following sub-command descriptions:

- ◆ [ip dhcp snooping information option encode no-subtype \(286\)](#)
- ◆ [ip dhcp snooping information option remote-id \(288\)](#)
- ◆ [ip dhcp snooping information option tr101 board-id \(289\)](#)

Syntax

ip dhcp snooping information option

no ip dhcp snooping information option

Default Setting

Option 82: Disabled

DHCP Snooping Information Option Sub-option Format: extra subtype included

DHCP Snooping Information Option Remote ID: MAC Address (hex encoded)

Command Mode

Global Configuration

Command Usage

- ◆ DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.

- ◆ When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server.
- ◆ When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- ◆ DHCP snooping must be enabled for the DHCP Option 82 information to be inserted into packets. When enabled, the switch will only add/remove option 82 information in incoming DHCP packets but not relay them. Packets are processed as follows:
 - If an incoming packet is a DHCP request packet with option 82 information, it will modify the option 82 information according to settings specified with `ip dhcp snooping information policy` command.
 - If an incoming packet is a DHCP request packet without option 82 information, enabling the DHCP snooping information option will add option 82 information to the packet.
 - If an incoming packet is a DHCP reply packet with option 82 information, enabling the DHCP snooping information option will remove option 82 information from the packet.

Example

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information option encode no-subtype

This command disables the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID) in Option 82 information generated by the switch. Use the **no** form to enable the use of these fields.

Syntax

[no] ip dhcp snooping information option encode no-subtype

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

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

Table 56: Option 82 information

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

The circuit identifier used by this switch starts at sub-option1 and goes to the end of the R-124 string. The R-124 string includes the following information:

- sub-type - Distinguishes different types of circuit IDs.
- sub-length - Length of the circuit ID type
- access node identifier - ASCII string. Default is the MAC address of the switch's CPU. This field is set by the [ip dhcp snooping information option](#) command,
- eth - The second field is the fixed string "eth"
- slot - The slot represents the stack unit for this system.
- port - The port which received the DHCP request. If the packet arrives over a trunk, the value is the ifIndex of the trunk.
- vlan - Tag of the VLAN which received the DHCP request.

Note that the sub-type and sub-length fields can be enabled or disabled using the [ip dhcp snooping information option](#) command.

- The **ip dhcp snooping information option circuit-id** command can be used to modify the default settings described above.
- ◆ The format for TR101 option 82 is: "<IP> eth <SID>/<PORT>[:<VLAN>]". Note that the SID (Switch ID) is always 0. By default the PVID is added to the end of the TR101 field for untagged packets. For tagged packets, the VLAN ID is always added.

Example

This example enables the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID).

```
Console(config)#no ip dhcp snooping information option encode no-subtype
Console(config)#
```

ip dhcp snooping information option remote-id This command sets the remote ID to the switch's IP address, MAC address, or arbitrary string, TR-101 compliant node identifier, or removes VLAN ID from the end of the TR101 field. Use the **no** form to restore the default setting.

Syntax

```
ip dhcp snooping information option remote-id  
  {ip-address [encode {ascii | hex}] |  
  mac-address [encode {ascii | hex}] | string string |  
  tr101 {node-identifier {ip | sysname} | no-vlan-field}
```

```
no ip dhcp snooping information option remote-id  
  [ip-address encode] | [mac-address encode] | [tr101 no-vlan-field]
```

mac-address - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch's CPU).

ip-address - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field.
(Range: 1-32 characters)

tr101 node-identifier - The remote ID generated by the switch is based on TR-101 syntax (R-124, Access_Node_ID).

ip - Specifies the switch's IP address as the node identifier.

sysname - Specifies the system name as the node identifier.

tr101 no-vlan-field - Do not add ":VLAN" in TR101 field for untagged packets.

Default Setting

DHCP Snooping Information Option Remote ID: MAC Address (hex encoded)
DHCP Snooping Information Option Remote ID TR101 VLAN Field: enabled

Command Mode

Global Configuration

Command Usage

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

Example

This example sets the remote ID to the switch's IP address.

```
Console(config)#ip dhcp snooping information option remote-id tr101
node-identifier ip
Console(config)#
```

ip dhcp snooping information option tr101 board-id

This command sets the board identifier used in Option 82 information based on TR-101 syntax. Use the **no** form to remove the board identifier.

Syntax

ip dhcp snooping information option tr101 board-id *board-id*

no ip dhcp snooping information option tr101 board-id

board-id – TR101 Board ID. (Range: 0-9)

Default Setting

not defined

Command Mode

Global Configuration

Example

This example sets the board ID to 0.

```
Console(config)#ip dhcp snooping information option tr101 board-id 0
Console(config)#
```

ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information. Use the **no** form to restore the default setting.

Syntax

ip dhcp snooping information policy {**drop** | **keep** | **replace**}

drop - Drops the client's request packet instead of relaying it.

keep - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

Default Setting

replace

Command Mode

Global Configuration

Command Usage

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

Example

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

Syntax

[no] ip dhcp snooping verify mac-address

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

Example

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

Related Commands

[ip dhcp snooping \(283\)](#)

[ip dhcp snooping vlan \(291\)](#)

[ip dhcp snooping trust \(294\)](#)

ip dhcp snooping vlan This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping vlan *vlan-id*

vlan-id - ID of a configured VLAN (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When DHCP snooping is enabled globally using the [ip dhcp snooping](#) command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the [ip dhcp snooping trust](#) command.
- ◆ When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- ◆ When DHCP snooping is globally enabled, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

Related Commands

[ip dhcp snooping \(283\)](#)

[ip dhcp snooping trust \(294\)](#)

ip dhcp snooping information option circuit-id

This command specifies DHCP Option 82 circuit-id suboption information. Use the **no** form to use the default settings.

Syntax

ip dhcp snooping information option circuit-id
{**string** *string* | {**tr101** {**node-identifier** {**ip** | **sysname**} |
no-vlan-field}

no dhcp snooping information option circuit-id [**tr101 no-vlan-field**]

string - An arbitrary string inserted into the circuit identifier field.
(Range: 1-32 characters)

tr101 node-identifier - The remote ID generated by the switch is based on TR-101 syntax (R-124, Access_Node_ID).

ip - Specifies the switch's IP address as the node identifier.

sysname - Specifies the system name as the node identifier.

tr101 no-vlan-field - Do not add ":VLAN" in TR101 field for untagged packets.

Default Setting

VLAN-Unit-Port

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. DHCP Option 82 allows compatible DHCP servers to use the information when assigning IP addresses, to set other services or policies for clients. For more information of this process, refer to the Command Usage section under the [ip dhcp snooping information option](#) command.
- ◆ Option 82 information generated by the switch is based on TR-101 syntax as shown below:

Table 57: Option 82 information

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

The circuit identifier used by this switch starts at sub-option1 and goes to the end of the R-124 string. The R-124 string includes the following information:

- sub-type - Distinguishes different types of circuit IDs.
- sub-length - Length of the circuit ID type

- access node identifier - ASCII string. Default is the MAC address of the switch's CPU. This field is set by the `ip dhcp snooping information option` command,
- eth - The second field is the fixed string "eth"
- slot - The slot represents the stack unit for this system.
- port - The port which received the DHCP request. If the packet arrives over a trunk, the value is the ifIndex of the trunk.
- vlan - Tag of the VLAN which received the DHCP request.

Note that the sub-type and sub-length fields can be enabled or disabled using the `ip dhcp snooping information option` command.

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

Example

This example sets the DHCP Snooping Information circuit-id suboption string.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping information option circuit-id string 4500
Console(config-if)#
```

ip dhcp snooping max-number This command configures the maximum number of DHCP clients which can be supported per interface. Use the **no** form to restore the default setting.

Syntax

ip dhcp snooping max-number *max-number*

no dhcp snooping max-number

max-number - Maximum number of DHCP clients. (Range: 1-32)

Default Setting

16

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets the maximum number of DHCP clients supported on port 1 to 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping max-number 2
Console(config-if)#
```

ip dhcp snooping trust This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping trust

Default Setting

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- ◆ Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- ◆ When DHCP snooping is enabled globally using the **ip dhcp snooping** command, and enabled on a VLAN with **ip dhcp snooping vlan** command, DHCP packet filtering will be performed on any untrusted ports within the

VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.

- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- ◆ *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

Example

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

Related Commands

[ip dhcp snooping \(283\)](#)

[ip dhcp snooping vlan \(291\)](#)

clear ip dhcp snooping binding

This command clears DHCP snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

Syntax

clear ip dhcp snooping binding *mac-address ip-address*

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

ip-address - Specifies the IP address bound to this entry.

Command Mode

Privileged Exec

Example

```
Console#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console#
```

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

Command Mode

Privileged Exec

Example

```
Console#clear ip dhcp snooping database flash
Console#
```

ip dhcp snooping database flash This command writes all dynamically learned snooping entries to flash memory.

Command Mode

Privileged Exec

Command Usage

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Example

```
Console#ip dhcp snooping database flash
Console#
```

show ip dhcp snooping This command shows the DHCP snooping configuration settings.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp snooping
Global DHCP Snooping Status: disabled
DHCP Snooping Information Option Status: disabled
DHCP Snooping Information Option Sub-option Format: extra subtype included
DHCP Snooping Information Option Remote ID: MAC Address (hex encoded)
DHCP Snooping Information Option Remote ID TR101 VLAN Field: enabled
DHCP Snooping Information Option TR101 Board ID: none
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:

Verify Source MAC-Address: enabled
```

Interface	Trusted	Max-Number	Circuit-ID Mode	Circuit-ID Value	Circuit-ID TR101 VLAN Field
Eth 1/1	No	16	VLAN-Unit-Port	---	enabled
Eth 1/2	No	16	VLAN-Unit-Port	---	enabled
Eth 1/3	No	16	VLAN-Unit-Port	---	enabled
Eth 1/4	No	16	VLAN-Unit-Port	---	enabled
Eth 1/5	No	16	VLAN-Unit-Port	---	enabled
.					
.					
.					

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

Command Mode
Privileged Exec

Example

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

IPv4 Source Guard

IPv4 Source Guard is a security feature that filters IPv4 traffic on network interfaces based on manually configured entries in the IPv4 Source Guard table, or dynamic entries in the DHCPv4 Snooping table when enabled (see [“DHCPv4 Snooping” on page 282](#)). IPv4 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv4 address of a neighbor to access the network. This section describes commands used to configure IPv4 Source Guard.

Table 58: IPv4 Source Guard Commands

Command	Function	Mode
ip source-guard binding	Adds a static address to the source-guard binding table	GC
ip source-guard	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC
ip source-guard max-binding	Sets the maximum number of entries that can be bound to an interface	IC
ip source-guard mode	Sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table	IC
clear ip source-guard binding blocked	Remove all blocked records	PE
show ip source-guard	Shows whether source guard is enabled or disabled on each interface	PE
show ip source-guard binding	Shows the source guard binding table	PE

ip source-guard binding This command adds a static address to the source-guard ACL or MAC address binding table. Use the **no** form to remove a static entry.

Syntax

ip source-guard binding [**mode** {**acl** | **mac**}] *mac-address*
vlan *vlan-id* *ip-address* **interface ethernet** *unit/port-list*

no ip source-guard binding [**mode** {**acl** | **mac**}] *mac-address* **vlan** *vlan-id*

mode - Specifies the binding mode.

acl - Adds binding to ACL table.

mac - Adds binding to MAC address table.

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN for an ACL filtering table or a range of VLANs for a MAC address filtering table. To specify a list separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-10/28)

Default Setting

No configured entries

Command Mode

Global Configuration

Command Usage

- ◆ If the binding mode is not specified in this command, the entry is bound to the ACL table by default.
- ◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.
- ◆ All static entries are configured with an infinite lease time, which is indicated with a value of zero by the [show ip source-guard](#) command (page 303).
- ◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.
- ◆ An entry with same MAC address and a different VLAN ID cannot be added to the binding table.

- ◆ Static bindings are processed as follows:
 - A valid static IP source guard entry will be added to the binding table in ACL mode if one of the following conditions is true:
 - If there is no binding entry with the same VLAN ID and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding.
 - If there is an entry with the same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
 - If there is an entry with the same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.
 - A valid static IP source guard entry will be added to the binding table in MAC mode if one of the following conditions are true:
 - If there is no binding entry with the same IP address and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding entry.
 - If there is a binding entry with same IP address and MAC address, then the new entry shall replace the old one.
- ◆ Only unicast addresses are accepted for static bindings.

Example

This example configures a static source-guard binding on port 5. Since the binding mode is not specified, the entry is bound to the ACL table by default.

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

Related Commands

[ip source-guard \(300\)](#)

[ip dhcp snooping \(283\)](#)

[ip dhcp snooping vlan \(291\)](#)

ip source-guard This command configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

Syntax

ip source-guard {sip | sip-mac}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- ◆ Setting source guard mode to “sip” or “sip-mac” enables this function on the selected port. Use the “sip” option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the “sip-mac” option to check these same parameters, plus the source MAC address. Use the **no ip source guard** command to disable this function on the selected port.
- ◆ When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.
- ◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier).
- ◆ Static addresses entered in the source guard binding table with the **ip source-guard binding** command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- ◆ If the IP source guard is enabled, an inbound packet’s IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- ◆ Filtering rules are implemented as follows:
 - If DHCPv4 snooping is disabled (see [page 283](#)), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for

the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

- If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
- If IP source guard is enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets allowed by DHCP snooping.
- Only unicast addresses are accepted for static bindings.

Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

Related Commands

[ip source-guard binding \(298\)](#)

[ip dhcp snooping \(283\)](#)

[ip dhcp snooping vlan \(291\)](#)

ip source-guard max-binding This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

Syntax

ip source-guard [mode {acl | mac}] max-binding *number*

no ip source-guard [mode {acl | mac}] max-binding

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL table.

mac - Searches for addresses in the MAC address table.

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-5 for ACL mode; 1-32 for MAC mode)

Default Setting

Mode: ACL, Maximum Binding: 5

Mode: MAC, Maximum Binding: 16

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command sets the maximum number of address entries that can be mapped to an interface in the binding table for the specified mode (ACL binding table or MAC address table) including dynamic entries discovered by DHCP snooping and static entries set by the `ip source-guard` command.
- ◆ The maximum binding for ACL mode restricts the number of “active” entries per port. If binding entries exceed the maximum number in IP source guard, only the maximum number of binding entries will be set. Dynamic binding entries exceeding the maximum number will be created but will not be active.
- ◆ The maximum binding for MAC mode restricts the number of MAC addresses learned per port. Authenticated IP traffic with different source MAC addresses cannot be learned if it would exceed this maximum number.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry. The mode is not specified, and therefore defaults to the ACL binding table.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

ip source-guard mode This command sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table. Use the **no** form to restore the default setting.

Syntax

ip source-guard mode {acl | mac}

no ip source-guard mode

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL binding table.

mac - Searches for addresses in the MAC address binding table.

Default Setting

ACL

Command Mode

Interface Configuration (Ethernet)

Command Usage

There are two modes for the filtering table:

- ◆ ACL - IP traffic will be forwarded if it passes the checking process in the ACL mode binding table.
- ◆ MAC - A MAC entry will be added in MAC address table if IP traffic passes the checking process in MAC mode binding table.

Example

This command sets the binding table mode for the specified interface to MAC mode:

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard mode mac
Console(config-if)#
```

clear ip source-guard binding blocked

This command clears source-guard binding table entries from RAM.

Syntax

clear ip source-guard binding blocked

Command Mode

Privileged Exec

Command Usage

When IP Source-Guard detects an invalid packet it creates a blocked record. These records can be viewed using the [show ip source-guard binding blocked](#) command. A maximum of 512 blocked records can be stored before the switch overwrites the oldest record with new blocked records. Use the **clear ip source-guard binding blocked** command to clear this table.

Example

This command clears the blocked record table.

```
Console(config)#clear ip source-guard binding blocked
Console(config)#
```

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard
```

Interface	Filter-type	Filter-table	ACL Table Max-binding	MAC Table Max-binding
Eth 1/1	DISABLED	ACL	5	1024
Eth 1/2	DISABLED	ACL	5	1024
Eth 1/3	DISABLED	ACL	5	1024
Eth 1/4	DISABLED	ACL	5	1024
Eth 1/5	DISABLED	ACL	5	1024
⋮				

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

Syntax

show ip source-guard binding [**dhcp-snooping** | **static** [**acl** | **mac**] | **blocked** [**vlan** *vlan-id* | **interface** *interface*]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see [page 282](#))

static - Shows static entries configured with the [ip source-guard binding](#) command.

acl - Shows static entries in the ACL binding table.

mac - Shows static entries in the MAC address binding table.

blocked - Shows MAC addresses which have been blocked by IP Source Guard.

vlan-id - ID of a configured VLAN (Range: 1-4094)

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard binding
```

MAC Address	IP Address	Type	VLAN	Interface
00-10-b5-f4-d0-01	10.2.44.96	static-acl	1	Eth 1/1

```
Console#
```


ARP Inspection

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

Table 59: ARP Inspection Commands

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

ip arp inspection This command enables ARP Inspection globally on the switch. Use the **no** form to disable this function.

Syntax

[no] ip arp inspection

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the **ip arp inspection vlan** command.
- ◆ When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- ◆ When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- ◆ When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- ◆ Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- ◆ When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection filter This command specifies an ARP ACL to apply to one or more VLANs. Use the **no** form to remove an ACL binding. Use the **no** form to remove an ACL binding.

Syntax

ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*} [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*}

arp-acl-name - Name of an ARP ACL. (Maximum length: 16 characters)

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

static - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

Default Setting

ARP ACLs are not bound to any VLAN

Static mode is not enabled

Command Mode

Global Configuration

Command Usage

- ◆ ARP ACLs are configured with the commands described [on page 344](#).
- ◆ If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.
- ◆ If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

Example

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection log-buffer logs This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the **no** form to restore the default settings.

Syntax

ip arp inspection log-buffer logs *message-number* **interval** *seconds*

no ip arp inspection log-buffer logs

message-number - The maximum number of entries saved in a log message.
(Range: 0-256, where 0 means no events are saved and no messages sent)

seconds - The interval at which log messages are sent. (Range: 0-86400)

Default Setting

Message Number: 20

Interval: 10 seconds

Command Mode

Global Configuration

Command Usage

- ◆ ARP Inspection must be enabled with the **ip arp inspection** command before this command will be accepted by the switch.
- ◆ By default, logging is active for ARP Inspection, and cannot be disabled.
- ◆ When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- ◆ If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- ◆ The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.
- ◆ The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

Example

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection validate This command specifies additional validation of address components in an ARP packet. Use the **no** form to restore the default setting.

Syntax

ip arp inspection validate
{**dst-mac** [**ip** [**allow-zeros**] [**src-mac**]] |
ip [**allow-zeros**] [**src-mac**]] | **src-mac**}

no ip arp inspection validate

dst-mac - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

allow-zeros - Allows sender IP address to be 0.0.0.0.

src-mac - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

Default Setting

No additional validation is performed

Command Mode

Global Configuration

Command Usage

By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

Example

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection vlan This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

Syntax

[no] ip arp inspection vlan {*vlan-id* | *vlan-range*}

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Setting

Disabled on all VLANs

Command Mode

Global Configuration

Command Usage

- ◆ When ARP Inspection is enabled globally with the **ip arp inspection** command, it becomes active only on those VLANs where it has been enabled with this command.
- ◆ When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- ◆ When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- ◆ When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- ◆ Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- ◆ When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit This command sets a rate limit for the ARP packets received on a port. Use the **no** form to restore the default setting.

Syntax

ip arp inspection limit {rate *pps* | **none**}

no ip arp inspection limit

pps - The maximum number of ARP packets that can be processed by the CPU per second on trusted or untrusted ports. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

none - There is no limit on the number of ARP packets that can be processed by the CPU.

Default Setting

15

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command applies to both trusted and untrusted ports.
- ◆ When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

ip arp inspection trust This command sets a port as trusted, and thus exempted from ARP Inspection. Use the **no** form to restore the default setting.

Syntax

[no] ip arp inspection trust

Default Setting

Untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration This command displays the global configuration settings for ARP Inspection.

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection configuration

ARP Inspection Global Information:

Global IP ARP Inspection Status : disabled
Log Message Interval           : 1 s
Log Message Number             : 5
Need Additional Validation(s)   : Yes
Additional Validation Type      : Destination MAC address
Console#
```

show ip arp inspection interface This command shows the trust status and ARP Inspection rate limit for ports.

Syntax

show ip arp inspection interface *[interface]*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection interface ethernet 1/1

Port Number      Trust Status      Rate Limit (pps)
-----
Eth 1/1          Trusted           150
Console#
```


show ip arp inspection log This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst MAC Address
--- --
1 1 11 192.168.2.2 192.168.2.1 00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

show ip arp inspection statistics This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection statistics

ARP packets received : 150
ARP packets dropped due to rate limit : 5
Total ARP packets processed by ARP Inspection : 150
ARP packets dropped by additional validation (source MAC address) : 0
ARP packets dropped by additional validation (destination MAC address) : 0
ARP packets dropped by additional validation (IP address) : 0
ARP packets dropped by ARP ACLs : 0
ARP packets dropped by DHCP snooping : 0

Console#
```

show ip arp inspection vlan This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

Syntax

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - Identifier for configured VLANs.

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection vlan 1
```

VLAN ID	DAI Status	ACL Name	ACL Status
1	disabled	sales	static

```
Console#
```

Denial of Service Protection

A denial-of-service attack (DoS attack) is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately.

This section describes commands used to protect against DoS attacks.

Table 60: DoS Protection Commands

Command	Function	Mode
dos-protection echo-charge	Protects against DoS echo/charge attacks	GC
dos-protection smurf	Protects against DoS smurf attacks	GC
dos-protection tcp-flooding	Protects against DoS TCP-flooding attacks	GC
dos-protection tcp-null-scan	Protects against DoS TCP-null-scan attacks	GC
dos-protection tcp-syn-fin-scan	Protects against DoS TCP-SYN/FIN-scan attacks	GC
dos-protection tcp-xmas-scan	Protects against DoS TCP-XMAS-scan attacks	GC
dos-protection udp-flooding	Protects against DoS UDP-flooding attacks	GC
dos-protection win-nuke	Protects against DoS WinNuke attacks	GC
show dos-protection	Shows the configuration settings for DoS protection	PE

dos-protection echo-charge

This command protects against DoS echo/charge attacks in which the echo service repeats anything sent to it, and the charge (character generator) service generates a continuous stream of data. When used together, they create an infinite loop and result in a denial-of-service. Use the **no** form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

Syntax

[no] dos-protection echo-charge [bit-rate-in-kilo rate]

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Setting

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection echo-charge bit-rate-in-kilo 65
Console(config)#
```

dos-protection smurf This command protects against DoS smurf attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should crash due to the many interrupts required to send ICMP Echo response packets. Use the **no** form to disable this feature.

Syntax**[no] dos-protection smurf****Default Setting**

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection smurf
Console(config)#
```

dos-protection tcp-flooding This command protects against DoS TCP-flooding attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. Use the **no** form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

Syntax**[no] dos-protection tcp-flooding [bit-rate-in-kilo rate]***rate* – Maximum allowed rate. (Range: 64-2000 kbits/second)**Default Setting**

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection tcp-flooding bit-rate-in-kilo 65  
Console(config)#
```

dos-protection tcp-null-scan

This command protects against DoS TCP-null-scan attacks in which a TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. Use the **no** form to disable this feature.

Syntax

[no] dos-protection tcp-null-scan

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection tcp-null-scan  
Console(config)#
```

dos-protection tcp-syn-fin-scan

This command protects against DoS TCP-SYN/FIN-scan attacks in which a TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. Use the **no** form to disable this feature.

Syntax

[no] dos-protection tcp-syn-fin-scan

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection syn-fin-scan
Console(config)#
```

dos-protection tcp-xmas-scan This command protects against DoS TCP-xmas-scan in which a so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. Use the **no** form to disable this feature.

Syntax

[no] dos-protection tcp-xmas-scan

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection tcp-xmas-scan
Console(config)#
```

dos-protection udp-flooding This command protects against DoS UDP-flooding attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. Use the **no** form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

Syntax

[no] dos-protection udp-flooding [bit-rate-in-kilo rate]

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Setting

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection udp-flooding bit-rate-in-kilo 65
Console(config)#
```

dos-protection win-uke This command protects against DoS WinNuke attacks in which affected the Microsoft Windows 3.1x/95/NT operating systems. In this type of attack, the perpetrator sends the string of OOB out-of-band (OOB) packets contained a TCP URG flag to the target computer on TCP port 139 (NetBIOS), casing it to lock up and display a “Blue Screen of Death.” This did not cause any damage to, or change data on, the computer’s hard disk, but any unsaved data would be lost. Microsoft made patches to prevent the WinNuke attack, but the OOB packets still put the service in a tight loop that consumed all available CPU time. Use the **no** form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

Syntax

[no] dos-protection win-uke [bit-rate-in-kilo rate]

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Setting

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection win-uke bit-rate-in-kilo65
Console(config)#
```

show dos-protection This command shows the configuration settings for the DoS protection commands.

Command Mode

Privileged Exec

Example

```
Console#show dos-protection
Global DoS Protection:

Echo/Chargen Attack      : Disabled, 1000 kilobits per second
Smurf Attack             : Enabled
TCP Flooding Attack      : Disabled, 1000 kilobits per second
TCP Null Scan            : Enabled
TCP SYN/FIN Scan         : Enabled
TCP XMAS Scan            : Enabled
UDP Flooding Attack      : Disabled, 1000 kilobits per second
```

```
WinNuke Attack          : Disabled, 1000 kilobits per second
Console#
```

Port-based Traffic Segmentation

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

Table 61: Commands for Configuring Traffic Segmentation

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

traffic-segmentation This command enables traffic segmentation. Use the **no** form to disable traffic segmentation.

Syntax

[no] traffic-segmentation

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.

- ◆ Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.
- ◆ When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 62: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured by the [traffic-segmentation uplink-to-uplink](#) command.

- ◆ When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.
- ◆ Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the [traffic-segmentation uplink/downlink](#) command.
- ◆ Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

Example

This example enables traffic segmentation globally on the switch.

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session This command creates a traffic-segmentation client session. Use the **no** form to remove a client session.

Syntax

[no] traffic-segmentation session *session-id*

session-id – Traffic segmentation session. (Range: 1-4)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use this command to create a new traffic-segmentation client session.
- ◆ Using the **no** form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

Example

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

traffic-segmentation uplink/downlink This command configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to remove a port from the segmented group.

Syntax

[no] traffic-segmentation [session session-id] {uplink interface-list [downlink interface-list] | downlink interface-list}

session-id – Traffic segmentation session. (Range: 1-4)

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

Session 1 if not defined

No segmented port groups are defined.

Command Mode

Global Configuration

Command Usage

- ◆ A port cannot be configured in both an uplink and downlink list.
- ◆ A port can only be assigned to one traffic-segmentation session.

- ◆ When specifying an uplink or downlink, a list of ports may be entered by using a hyphen or comma in the *port* field. Note that lists are not supported for the *channel-id* field.
- ◆ A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- ◆ If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

Example

This example enables traffic segmentation, and then sets port 10 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
downlink ethernet 1/5-8
Console(config)#
```

traffic-segmentation uplink-to-uplink This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the **no** form to restore the default.

Syntax

[no] traffic-segmentation uplink-to-uplink {blocking | forwarding}

blocking – Blocks traffic between uplink ports assigned to different sessions.

forwarding – Forwards traffic between uplink ports assigned to different sessions.

Default Setting

Blocking

Command Mode

Global Configuration

Example

This example enables forwarding of traffic between uplink ports assigned to different client sessions.

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```

show traffic-segmentation This command displays the configured traffic segments.

Command Mode
Privileged Exec

Example

```
Console#show traffic-segmentation
```

```
Traffic segmentation Status :      Disabled
Uplink-to-Uplink Mode       :      Forwarding
```

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

```
Console#
```


Access Control Lists

Access Control Lists (ACL) provide ingress packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header type), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 63: Access Control List Commands

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

IPv4 ACLs

The commands in this section configure ingress ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 64: IPv4 ACL Commands

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

access-list ip This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list ip {standard | extended} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 128 rules.

Example

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

Related Commands

[permit, deny \(326\)](#)

[show ip access-list \(331\)](#)

permit, deny (Standard IP ACL) This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

{permit | deny} {any | *source bitmask* | host *source*}
[time-range *time-range-name*]

no {permit | deny} {any | *source bitmask* | host *source*}

any – Any source IP address.

source – Source IP address.

bitmask – Dotted decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

time-range-name - Name of the time range. (Range: 1-16 characters)

Default Setting

None

Command Mode

Standard IPv4 ACL

Command Usage

- ◆ New rules are appended to the end of the list.
- ◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

[access-list ip \(326\)](#)

[Time Range \(149\)](#)

permit, deny (Extended IPv4 ACL) This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} [protocol-number | udp]
  {any | source address-bitmask | host source}
  {any | destination address-bitmask | host destination}
  [dscp dscp] [precedence precedence]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
  [time-range time-range-name]
```

```
no {permit | deny} [protocol-number | udp]  
    {any | source address-bitmask | host source}  
    {any | destination address-bitmask | host destination}  
    [dscp dscp] [precedence precedence]  
    [source-port sport [bitmask]]  
    [destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp  
    {any | source address-bitmask | host source}  
    {any | destination address-bitmask | host destination}  
    [dscp dscp] [precedence precedence]  
    [source-port sport [bitmask]]  
    [destination-port dport [port-bitmask]]  
    [control-flag control-flags flag-bitmask]  
    [time-range time-range-name]
```

```
no {permit | deny} tcp  
    {any | source address-bitmask | host source}  
    {any | destination address-bitmask | host destination}  
    [dscp dscp] [precedence precedence]  
    [source-port sport [bitmask]]  
    [destination-port dport [port-bitmask]]  
    [control-flag control-flags flag-bitmask]
```

protocol-number – A specific protocol number. (Range: 0-255)

source – Source IP address.

destination – Destination IP address.

address-bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

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

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

sport – Protocol⁴ source port number. (Range: 0-65535)

dport – Protocol⁴ destination port number. (Range: 0-65535)

port-bitmask – Decimal number representing the port bits to match.
(Range: 0-65535)

control-flags – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

flag-bitmask – Decimal number representing the code bits to match.

time-range-name - Name of the time range. (Range: 1-16 characters)

Default Setting

None

Command Mode

Extended IPv4 ACL

4. Includes TCP, UDP or other protocol types.

Command Usage

- ◆ All new rules are appended to the end of the list.
- ◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- ◆ The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”
 - Both SYN and ACK valid, use “control-code 18 18”
 - SYN valid and ACK invalid, use “control-code 2 18”
- ◆ If an Extended IPv4 rule and MAC rule match the same packet, and these rules specify a “permit” entry and “deny” entry, the “deny” action takes precedence.

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any destination-
port 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-  
flag 2 2  
Console(config-ext-acl)#
```

Related Commands

[access-list ip \(326\)](#)

[Time Range \(149\)](#)

ip access-group This command binds an IPv4 ACL to a port. Use the **no** form to remove the port.

Syntax

ip access-group *acl-name* **in**
[**time-range** *time-range-name*] [**counter**]

no ip access-group *acl-name* **in**

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

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-32 characters)

counter – Enables counter for ACL statistics.



Note: ACLs cannot be applied to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2  
Console(config-if)#ip access-group david in  
Console(config-if)#
```

Related Commands

[show ip access-list \(331\)](#)

[Time Range \(149\)](#)

show ip access-group This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
  IP access-list david in
Console#
```

show ip access-list This command displays the rules for configured IPv4 ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IP ACL.

extended – Specifies an extended IP ACL.

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

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands

[permit, deny \(326\)](#)

IPv6 ACLs

The commands in this section configure ingress ACLs based on IPv6 addresses, DSCP traffic class, or next header type. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 65: IPv6 ACL Commands

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

access-list ipv6 This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list ipv6 {standard | extended} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.

- ◆ An ACL can contain up to 64 rules.

Example

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

Related Commands

[permit, deny \(Standard IPv6 ACL\) \(333\)](#)

[permit, deny \(Extended IPv6 ACL\) \(334\)](#)

[ipv6 access-group \(337\)](#)

[show ipv6 access-list \(338\)](#)

permit, deny (Standard IPv6 ACL) This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} {any | host source-ipv6-address |  
  source-ipv6-address/prefix-length}  
[time-range time-range-name]
```

```
no {permit | deny} {any | host source-ipv6-address |  
  source-ipv6-address/prefix-length}
```

any – Any source IP address.

host – Keyword followed by a specific IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

time-range-name - Name of the time range. (Range: 1-32 characters)

Default Setting

None

Command Mode

Standard IPv6 ACL

Command Usage

New rules are appended to the end of the list.

Example

This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

Related Commands

[access-list ipv6 \(332\)](#)

[Time Range \(149\)](#)

permit, deny (Extended IPv6 ACL) This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, or next header type. Use the **no** form to remove a rule.

Syntax

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

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

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific source IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 128 bits of the destination address.)

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 for source prefix, 0-128 for destination prefix)

dscp - DSCP traffic class. (Range: 0-63)

next-header - Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

sport - Protocol⁵ source port number. (Range: 0-65535)

dport - Protocol⁴ destination port number. (Range: 0-65535)

port-bitmask - Decimal number representing the port bits to match. (Range: 0-65535)

time-range-name - Name of the time range. (Range: 1-32 characters)

Default Setting

None

Command Mode

Extended IPv6 ACL

Command Usage

- ◆ All new rules are appended to the end of the list.
- ◆ Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

0	: Hop-by-Hop Options	(RFC 2460)
6	: TCP Upper-layer Header	(RFC 1700)
17	: UDP Upper-layer Header	(RFC 1700)
43	: Routing	(RFC 2460)
44	: Fragment	(RFC 2460)
51	: Authentication	(RFC 2402)
50	: Encapsulating Security Payload	(RFC 2406)
60	: Destination Options	(RFC 2460)

Example

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

```
Console(config-ext-ipv6-acl)#permit any 2009:db90:2229::79/8
Console(config-ext-ipv6-acl)#
```

5. Includes TCP and UDP.

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent from any source to any destination when the next header is 43."

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

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

```
Set ACL
Console(config)#access-list ipv6 extended snmp-acl
Console(config-ext-acl)#permit any any destination-port 161
Console(config-ext-acl)#permit any any destination-port 162
Console(config-ext-acl)#exit

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

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

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

Related Commands

[access-list ipv6 \(332\)](#)

[Time Range \(149\)](#)

ipv6 access-group This command binds an IPv6 ACL to a port. Use the **no** form to remove the port.

Syntax

ipv6 access-group *acl-name* **in**
[*time-range time-range-name*] [**counter**]

no ipv6 access-group *acl-name* **in**

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

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-32 characters)

counter – Enables counter for ACL statistics.



Note: IPv6 ACLs cannot be applied to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

Related Commands

[show ipv6 access-list \(338\)](#)

[Time Range \(149\)](#)

show ipv6 access-group This command shows the ports assigned to IPv6 ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-group
Interface ethernet 1/2
  IPv6 standard access-list david in
Console#
```

Related Commands

[ipv6 access-group \(337\)](#)

show ipv6 access-list This command displays the rules for configured IPv6 ACLs.

Syntax

show ipv6 access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IPv6 ACL.

extended – Specifies an extended IPv6 ACL.

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

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

Related Commands

[permit, deny \(Standard IPv6 ACL\) \(333\)](#)

[permit, deny \(Extended IPv6 ACL\) \(334\)](#)

[ipv6 access-group \(337\)](#)

MAC ACLs

The commands in this section configure ingress ACLs based on hardware addresses, packet format, and Ethernet type. The ACLs can further specify optional IP and IPv6 addresses including protocol type and upper layer ports. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 66: MAC ACL Commands

Command	Function	Mode
access-list mac	Creates a MAC ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type. They can be further specified using optional IP and IPv6 addresses including protocol type and upper layer ports.	MAC-ACL
mac access-group	Binds a MAC ACL to a port	IC

Table 66: MAC ACL Commands (Continued)

Command	Function	Mode
show mac access-group	Shows port assignments for MAC ACLs	PE
show mac access-list	Displays the rules for configured MAC ACLs	PE

access-list mac This command enters MAC ACL configuration mode. Rules can be added to filter packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Rules can also be used to filter packets based on IPv4/v6 addresses, including Layer 4 ports and protocol types. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list mac *acl-name*

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 128 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

[permit, deny \(340\)](#)

[mac access-group \(342\)](#)

[show mac access-list \(343\)](#)

permit, deny (MAC ACL) This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Rules can also filter packets based on IPv4/v6 addresses, including Layer 4 ports and protocol types. Use the **no** form to remove a rule.

Syntax

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



Note: The default is for Ethernet II packets.

```
{permit | deny} tagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [cos cos cos-bitmask] [vid vid vid-bitmask]  
  [ethertype ethertype [ethertype-bitmask]]  
  [time-range time-range-name]  
  
no {permit | deny} tagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [cos cos cos-bitmask] [vid vid vid-bitmask]  
  [ethertype ethertype [ethertype-bitmask]]  
  
{permit | deny} untagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [ethertype ethertype [ethertype-bitmask]]  
  [time-range time-range-name]  
  
no {permit | deny} untagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [ethertype ethertype [ethertype-bitmask]]  
  
{permit | deny} tagged-802.3  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [cos cos cos-bitmask] [vid vid vid-bitmask]  
  [time-range time-range-name]  
  
no {permit | deny} tagged-802.3  
  {any | host source | source address-bitmask}
```

{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]

{permit | deny} untagged-802.3

{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**time-range** *time-range-name*]

no {permit | deny} untagged-802.3

{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

tagged-eth2 – Tagged Ethernet II packets.

untagged-eth2 – Untagged Ethernet II packets.

tagged-802.3 – Tagged Ethernet 802.3 packets.

untagged-802.3 – Untagged Ethernet 802.3 packets.

any – Any MAC, IPv4 or IPv6 source or destination address.

host – A specific MAC, IPv4 or IPv6 address.

source – Source MAC, IPv4 or IPv6 address.

destination – Destination MAC, IPv4 or IPv6 address.

*address-bitmask*⁶ – Bitmask for MAC address (in hexadecimal format).

network-mask – Network mask for IP subnet. This mask identifies the host address bits used for routing to specific subnets.

prefix-length – Length of IPv6 prefix. A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

cos – Class-of-Service value (Range: 0-7)

*cos-bitmask*⁶ – Class-of-Service bitmask. (Range: 0-7)

vid – VLAN ID. (Range: 1-4094)

*vid-bitmask*⁶ – VLAN bitmask. (Range: 1-4095)

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

*ethertype-bitmask*⁶ – Protocol bitmask. (Range: 0-ffff hex)

time-range-name – Name of the time range. (Range: 1-32 characters)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- ◆ New rules are added to the end of the list.

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

- ◆ The **ethertype** option can only be used to filter Ethernet II formatted packets.
- ◆ A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
 - 0800 - IP
 - 0806 - ARP
 - 8137 - IPX
- ◆ If an Extended IPv4 rule and MAC rule match the same packet, and these rules specify a “permit” entry and “deny” entry, the “deny” action takes precedence.

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

[access-list mac \(339\)](#)

[Time Range \(149\)](#)

mac access-group This command binds a MAC ACL to a port. Use the **no** form to remove the port.

Syntax

mac access-group *acl-name* **in**
[**time-range** *time-range-name*] [**counter**]

no mac access-group *acl-name* **in**

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

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-32 characters)

counter – Enables counter for ACL statistics.



Note: MAC ACLs cannot be applied to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

[show mac access-list \(343\)](#)

[Time Range \(149\)](#)

show mac access-group This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
MAC access-list M5 in
Console#
```

Related Commands

[mac access-group \(342\)](#)

show mac access-list This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list *[acl-name]*

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

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

[permit, deny \(340\)](#)

[mac access-group \(342\)](#)

ARP ACLs

The commands in this section configure ingress ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the [ip arp inspection vlan](#) command.

Table 67: ARP ACL Commands

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

access-list arp This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list arp *acl-name*

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 128 rules.

Example

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

Related Commands

[permit, deny \(345\)](#)[show access-list arp \(346\)](#)

permit, deny (ARP ACL) This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

Syntax

```
[no] {permit | deny} ip
    {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

This form indicates either request or response packets.

```
[no] {permit | deny} request
    ip {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

```
[no] {permit | deny} response
    ip {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

source-ip – Source IP address.

destination-ip – Destination IP address with bitmask.

*ip-address-bitmask*⁷ – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

*mac-address-bitmask*⁷ – Bitmask for MAC address (in hexadecimal format).

log - Logs a packet when it matches the access control entry.

Default Setting

None

7. For all bitmasks, binary “1” means relevant and “0” means ignore.

Command Mode

ARP ACL

Command Usage

New rules are added to the end of the list.

Example

This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac  
any any  
Console(config-mac-acl)#
```

Related Commands

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

show access-list arp This command displays the rules for configured ARP ACLs.

Syntax

show access-list arp [*acl-name*]

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

Command Mode

Privileged Exec

Example

```
Console#show access-list arp  
ARP access-list factory:  
  permit response ip any 192.168.0.0 255.255.0.0 mac any any  
Console#
```

Related Commands

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

ACL Information

This section describes commands used to display ACL information.

Table 68: ACL Information Commands

Command	Function	Mode
<code>clear access-list hardware counters</code>	Clears hit counter for rules in all ACLs, or in a specified ACL	PE
<code>show access-group</code>	Shows the ACLs assigned to each port	PE
<code>show access-list</code>	Show all ACLs and associated rules	PE

clear access-list hardware counters This command clears the hit counter for the rules in all ACLs, or for the rules in a specified ACL.

Syntax

clear access-list hardware counters

[direction in [interface *interface*]] |
[interface *interface*] | [name *acl-name*]

in – Clears counter for ingress rules.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

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

Command Mode

Privileged Exec

Example

```
Console#clear access-list hardware counters
Console#
```

show access-group This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
```

```
IP access-list david
MAC access-list jerry
Console#
```

show access-list This command shows all ACLs and associated rules.

Syntax

show access-list

```
[[arp acl-name]] |
[ip [extended acl-name] | standard acl-name]] |
[ipv6 [extended acl-name] | standard acl-name]] |
[mac acl-name]] | [tcam-utilization] | [hardware counters]]
```

arp – Shows ingress rules for ARP ACLs.

hardware counters – Shows statistics for all ACLs.⁸

ip extended – Shows ingress rules for Extended IPv4 ACLs.

ip standard – Shows ingress rules for Standard IPv4 ACLs.

ipv6 extended – Shows ingress rules for Extended IPv6 ACLs.

ipv6 standard – Shows ingress rules for Standard IPv6 ACLs.

mac – Shows ingress for MAC ACLs.

tcam-utilization – Shows the percentage of user configured ACL rules as a percentage of total ACL rules

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

Command Mode

Privileged Exec

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
Console#
```

8. Due to a hardware limitation, this option only displays statistics for permit rules.

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

Table 69: Interface Commands

Command	Function	Mode
<i>Interface Configuration</i>		
<code>interface</code>	Configures an interface type and enters interface configuration mode	GC
<code>capabilities</code>	Advertises the capabilities of a given interface for use in autonegotiation	IC
<code>description</code>	Adds a description to an interface configuration	IC
<code>flowcontrol</code>	Enables flow control on a given interface	IC
<code>history</code>	Configures a periodic sampling of statistics, specifying the sampling interval and number of samples	IC
<code>media-type</code>	Forces transceiver mode to use for SFP ports	IC
<code>negotiation</code>	Enables autonegotiation of a given interface	IC
<code>shutdown</code>	Disables an interface	IC
<code>speed-duplex</code>	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
<code>clear counters</code>	Clears statistics on an interface	PE
<code>show interfaces brief</code>	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
<code>show interfaces counters</code>	Displays statistics for the specified interfaces	NE, PE
<code>show interfaces history</code>	Displays periodic sampling of statistics, including the sampling interval, number of samples, and counter values	NE, PE
<code>show interfaces status</code>	Displays status for the specified interface	NE, PE
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE
<i>Transceiver Threshold Configuration</i>		
<code>transceiver-monitor</code>	Sends a trap when any of the transceiver's operational values fall outside specified thresholds	IC
<code>transceiver-threshold-auto</code>	Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent	IC
<code>transceiver-threshold current</code>	Sets thresholds for transceiver current which can be used to trigger an alarm or warning message	IC

Table 69: Interface Commands (Continued)

Command	Function	Mode
transceiver-threshold rx-power	Sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message	IC
transceiver-threshold temperature	Sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message	IC
transceiver-threshold tx-power	Sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message	IC
transceiver-threshold voltage	Sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message	IC
show interfaces transceiver	Displays the temperature, voltage, bias current, transmit power, and receive power	PE
show interfaces transceiver-threshold	Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power	PE
<i>Cable Diagnostics</i>		
test cable-diagnostics	Performs cable diagnostics on the specified port	PE
show cable-diagnostics	Shows the results of a cable diagnostics test	PE
<i>Power Savings</i>		
power-save	Enables power savings mode on the specified port	IC
show power-save	Shows the configuration settings for power savings	PE

Interface Configuration

interface This command configures an interface type and enters interface configuration mode. Use the **no** form with a trunk to remove an inactive interface. Use the **no** form with a Layer 3 VLAN (normal type) to change it back to a Layer 2 interface.



Note: A VLAN must first be configured using the [vlan database](#) command before its VLAN interface can be entered. Other interface types do not need to be configured beforehand.

Note: The switch supports a maximum binding of 8 addresses to a VLAN interface. The 8 is shared between IPv4 and IPv6. If 6 IPv4 addresses are bound to the VLAN interface, only two IPv6 address could be bound.

Syntax

```
[no] interface interface
      interface
      ethernet unit/port-list
              unit - Unit identifier. (Range: 1)
```

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify several different ports, enter the following command:

```
Console(config)#interface ethernet 1/17-20,23
Console(config-if)#
```

capabilities This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[no] capabilities {1000full | 100full | 100half | 10full | 10half | flowcontrol}

1000full - Supports 1 Gbps full-duplex operation

100full - Supports 100 Mbps full-duplex operation

100half - Supports 100 Mbps half-duplex operation

10full - Supports 10 Mbps full-duplex operation

10half - Supports 10 Mbps half-duplex operation

flowcontrol - Supports flow control

Default Setting

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/LHX/ZX (SFP): 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When auto-negotiation is enabled with the [negotiation](#) command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the [speed-duplex](#) and [flowcontrol](#) commands.

Example

The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

[negotiation \(355\)](#)

[speed-duplex \(356\)](#)

[flowcontrol \(353\)](#)

description This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The description is displayed by the [show interfaces status](#) command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```


flowcontrol This command enables flow control. Use the **no** form to disable flow control.

Syntax

[no] flowcontrol

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- ◆ Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.
- ◆ To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- ◆ When using the [negotiation](#) command to enable auto-negotiation, the optimal settings will be determined by the [capabilities](#) command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

[negotiation \(355\)](#)

[capabilities \(351\)](#)

history This command configures a periodic sampling of statistics, specifying the sampling interval and number of samples. Use the **no** form to remove a named entry from the sampling table.

Syntax

history *name interval buckets*

no history *name*

name - A symbolic name for this entry in the sampling table. (Range: 1-32 characters)

interval - The interval for sampling statistics. (Range: 1-1440 minutes.

buckets - The number of samples to take. (Range: 1-96)

Default Setting

15min - 15 minute interval, 96 buckets

1day - 1 day interval, 7 buckets

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets a interval of 15 minutes for sampling standard statistical values on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#history 15min 15 10
Console(config-if)#
```

media-type This command forces the transceiver mode to use for SFP ports. Use the **no** form to restore the default mode.

Syntax

media-type {**sfp-forced** [*mode*]}

no media-type

sfp-forced - Forces transceiver mode for the SFP port.

mode

1000sfp - Always uses 1000BASE SFP mode.

100fx - Always uses 100BASE-FX mode.

Default Setting

SFP ports: None

Command Mode

Interface Configuration (Ethernet)

Example

This forces the switch to use the 1000sfp mode for SFP port 28.

```
Console(config)#interface ethernet 1/28
Console(config-if)#media-type sfp-forced 1000sfp
Console(config-if)#
```

negotiation This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

Syntax

[no] negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- ◆ When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the [capabilities](#) command. When auto-negotiation is disabled, you must manually specify the link attributes with the [speed-duplex](#) and [flowcontrol](#) commands.
- ◆ If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 10 to use auto-negotiation.

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

[capabilities \(351\)](#)

[speed-duplex \(356\)](#)

shutdown This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[no] shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

speed-duplex This command configures the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {100full | 100half | 10full | 10half}

no speed-duplex

100full - Forces 100 Mbps full-duplex operation

100half - Forces 100 Mbps half-duplex operation

10full - Forces 10 Mbps full-duplex operation

10half - Forces 10 Mbps half-duplex operation

Default Setting

- ◆ Auto-negotiation is enabled by default.
- ◆ When auto-negotiation is disabled, the default speed-duplex setting is **100full** for 1000BASE-T ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- ◆ To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- ◆ When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

[negotiation \(355\)](#)

[capabilities \(351\)](#)

clear counters This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces brief This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

Command Mode

Privileged Exec

Command Usage

- ◆ If an SFP transceiver is inserted in a port, the Type field will show the SFP type as interpreted from Ethernet Compliance Codes (Data Byte 6 in Address A0h). The Ethernet Compliance Code is a bitmap value, of which one bit is supposedly turned on. However, if the read-out is not recognizable (e.g., 2 or more bits on, or all 0s), the Type field just displays the raw data (hexadecimal value).
- ◆ The Type field will always display “NA” for a trunk entry because a trunk allows for mixed port types such as 1000BASE-T and 1000BASE SFP.

Example

```
Console#show interfaces brief
Interface Name      Status    PVID Pri Speed/Duplex  Type           Trunk
-----
Eth 1/ 1           Down      1   0 Auto        1000BASE-T     None
Eth 1/ 2           Down      1   0 Auto        1000BASE-T     None
Eth 1/ 3           Down      1   0 Auto        1000BASE-T     None
Eth 1/ 4           Down      1   0 Auto        1000BASE-T     None
Eth 1/ 5           Down      1   0 Auto        1000BASE-T     None
Eth 1/ 6           Down      1   0 Auto        1000BASE-T     None
⋮
```

If there are trunks configured, the **show interface brief** command will list them:

```
Console#show interfaces brief
```

```
Vty-1# show interfaces brief
```

Interface	Name	Status	PVID	Pri	Speed/Duplex	Type	Trunk
Eth 1/ 1	StaticTrunk3	Up	1	0	Auto-1000full	1000BASE-T	3
Eth 1/ 2	StaticTrunk3	Up	1	0	Auto-1000full	1000BASE-T	3
Eth 1/ 3	StaticTrunk3	Up	1	0	Auto-1000full	1000BASE-T	3
Eth 1/ 4	StaticTrunk3	Up	1	0	Auto-1000full	1000BASE-T	3
Eth 1/ 5		Down	1	0	Auto	1000BASE-T	None
Eth 1/ 6	DynamicTrunk1	Up	1	0	Auto-1000full	1000BASE-T	1
Eth 1/ 7		Down	1	0	Auto	1000BASE-T	None
Eth 1/ 8	DynamicTrunk1	Up	1	0	Auto-1000full	1000BASE-T	1
Eth 1/ 9		Down	1	0	Auto	1000BASE-T	None
Eth 1/10	DynamicTrunk1	Up	1	0	Auto-1000full	1000BASE-T	1
Eth 1/11		Down	1	0	Auto	1000BASE-T	None
~							
Eth 1/28		Down	1	0	Auto	1000BASE SFP	None
Trunk 1	DynamicTrunk1	Up	1	0	Auto-1000full	1000BASE-T	1
Trunk 3	StaticTrunk3	Up	1	0	Auto-1000full	1000BASE-T	3

show interfaces counters This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces counters ethernet 1/1
Ethernet 1/ 1
===== IF table Stats =====
      2166458 Octets Input
    14734059 Octets Output
      14707 Unicast Input
      19806 Unicast Output
         0 Discard Input
         0 Discard Output
```

```

0 Error Input
===== Extended Iftable Stats =====
23 Multi-cast Input
5525 Multi-cast Output
170 Broadcast Input
11 Broadcast Output
===== Ether-like Stats =====
0 FCS Errors
0 Single Collision Frames
0 Multiple Collision Frames
0 Deferred Transmissions
0 Late Collisions
0 Excessive Collisions
0 Internal Mac Transmit Errors
0 Frames Too Long
0 Symbol Errors
0 Pause Frames Input
0 Pause Frames Output
===== RMON Stats =====
0 Drop Events
16900558 Octets
40243 Packets
170 Broadcast PKTS
23 Multi-cast PKTS
0 Undersize PKTS
0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
5271 Packet Size <= 64 Octets
3589 Packet Size 65 to 127 Octets
222 Packet Size 128 to 255 Octets
313 Packet Size 256 to 511 Octets
190 Packet Size 512 to 1023 Octets
444 Packet Size 1024 to 1518 Octets
===== Port Utilization =====
111 Octets Input in kbits per second
0 Packets Input per second
0.00 % Input Utilization
606 Octets Output in kbits per second
1 Packets Output per second
0.00 % Output Utilization

Console#

```

Table 70: show interfaces counters - display description

Parameter	Description
<i>IF Table Stats</i>	
Octets Input	The total number of octets received on the interface, including framing characters.
Octets Output	The total number of octets transmitted out of the interface, including framing characters.
Unicast Input	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Unicast Output	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Table 70: show interfaces counters - display description (Continued)

Parameter	Description
Discard Input	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Discard Output	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Error Input	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
<i>Extended IF Table Stats</i>	
Multicast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Multicast Output	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Broadcast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Broadcast Output	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
<i>Etherlike Statistics</i>	
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.

Table 70: show interfaces counters - display description (Continued)

Parameter	Description
Symbol Errors	<p>For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present.</p> <p>For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII.</p> <p>For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII</p>
<i>RMON Statistics</i>	
Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
<i>CRC Align Errors</i>	
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received and transmitted that were less than 64 octets in length (excluding framing bits but including FCS octets).
65-127 Octets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
128-255 Octets	
256-511 Octets	
512-1023 Octets	
1024-1518 Octets	
<i>Utilization Statistics</i>	
Octets input per second	Number of octets entering this interface in kbits per second.
Packets input per second	Number of packets entering this interface in packets per second.
Input utilization	The input utilization rate for this interface.

Table 70: show interfaces counters - display description (Continued)

Parameter	Description
Octets output per second	Number of octets leaving this interface in kbits per second.
Packets output per second	Number of packets leaving this interface in packets per second.
Output utilization	The output utilization rate for this interface.

show interfaces history This command displays periodic sampling of statistics, including the sampling interval, number of samples, and counter values.

Syntax

show interfaces history [*interface* [*name* **current** | **previous** *index count*]
[**input** | **output**]]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

name - Name of sample as defined in the [history](#) command.
(Range: 1-32 characters)

current - Statistics recorded in current interval.

previous - Statistics recorded in previous intervals.

index - An index into the buckets containing previous samples.
(Range: 1-96)

count - The number of historical samples to display. (Range: 1-96)

input - Ingress traffic.

output - Egress traffic.

Default Setting

Shows the historical settings and status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces history ethernet 1/1 15min
Interface      : Eth 1/ 1
Name           : 15min
```

```
Interval          : 900 second(s)
Buckets Requested : 96
Buckets Granted   : 1
Status            : Active

Current Entries

Start Time  %      Octets Input  Unicast      Multicast      Broadcast
-----
00d 00:15:04  0.00          72675        524           35             41

Errors
-----
0

%      Octets Output  Unicast      Multicast      Broadcast
-----
0.00          513760        653           336             0

Discards
-----
0

Previous Entries

Start Time  %      Octets Input  Unicast      Multicast      Broadcast
-----
00d 00:00:03  0.66      80758067     106273        619717         69176

Start Time  Discards      Errors
-----
00d 00:00:03      69176          2

Start Time  %      Octets Output  Unicast      Multicast      Broadcast
-----
00d 00:00:03  0.00          677855        705           445             14

Start Time  Discards
-----
00d 00:00:03      0
Console#
```

show interfaces status This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```

Console#show interfaces status ethernet 1/1
Information of Eth 1/1
Basic Information:
  Port Type           : 1000BASE-T
  MAC Address         : 00-E0-0C-00-00-FE
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : Auto
  Capabilities        : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 500 packets/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 500 packets/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Flow Control        : Disabled
  LACP                : Disabled
  MAC Learning        : Enabled
  Link-up-down Trap   : Enabled
Current Status:
  Link Status         : Up
  Port Operation Status : Up
  Operation Speed-duplex : 100full
  Up Time             : 0w 0d 1h 11m 2s (4262 seconds)
  Flow Control Type    : None
  Max Frame Size       : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status  : Enabled
Console#

```

show interfaces switchport This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 1.

```
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
Broadcast Threshold           : Enabled, 500 packets/second
Multicast Threshold           : Disabled
Unknown Unicast Threshold     : Disabled
LACP Status                   : Disabled
Ingress Rate Limit            : Disabled, 1000M bits per second
Egress Rate Limit             : Disabled, 1000M bits per second
VLAN Membership Mode          : Hybrid
Ingress Rule                   : Disabled
Acceptable Frame Type         : All frames
Native VLAN                   : 1
Priority for Untagged Traffic  : 0
Allowed VLAN                   : 1(u)
802.1Q Tunnel Status          : Disabled
802.1Q Tunnel Mode            : Normal
802.1Q Tunnel TPID            : 8100 (Hex)
Console#
```

Table 71: show interfaces switchport - display description

Field	Description
Broadcast Threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 416).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 416).
Unknown Unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 416).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 383).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 1023).

Table 71: show interfaces switchport - display description (Continued)

Field	Description
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 468).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 467).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 465).
Native VLAN	Indicates the default Port VLAN ID (page 469).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 492).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 465).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 472).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 474).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 473).

Transceiver Threshold Configuration

transceiver-monitor This command sends a trap when any of the transceiver's operational values fall outside of specified thresholds. Use the **no** form to disable trap messages.

Syntax

transceiver-monitor

Default Setting

Disabled

Command Mode

Interface Configuration (SFP Ports)

Example

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-monitor
Console#
```

transceiver-threshold-auto This command uses default threshold settings obtained from the transceiver to determine when an alarm or warning message should be sent. Use the **no** form to disable this feature.

Syntax

transceiver-threshold-auto

Default Setting

Enabled

Command Mode

Interface Configuration (SFP Ports)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold-auto
Console#
```

transceiver-threshold-current This command sets thresholds for transceiver current which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold current {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high current threshold for an alarm message.

high-warning – Sets the high current threshold for a warning message.

low-alarm – Sets the low current threshold for an alarm message.

low-warning – Sets the low current threshold for a warning message.

threshold-value – The threshold of the transceiver current.

(Range: 0-13100 in units of 0.01 mA)

Default Setting

High Alarm: 100 mA

High Warning: 90 mA

Low Warning: 7 mA

Low Alarm: 6 mA

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ If trap messages are enabled with the [transceiver-monitor](#) command, and a high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the

threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.

- ◆ If trap messages are enabled with the [transceiver-monitor](#) command, and a low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- ◆ Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver current at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold current low-alarm 100
Console(config-if)#transceiver-threshold rx-power high-alarm 700
Console#
```

transceiver-threshold rx-power This command sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold rx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the received signal.

(Range: -4000 - 820 in units of 0.01 dBm)

Default Setting

High Alarm: -3.00 dBm

High Warning: -3.50 dBm

Low Warning: -21.00 dBm

Low Alarm: -21.50 dBm

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the signal power received at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold rx-power low-alarm -21
Console(config-if)#transceiver-threshold rx-power high-alarm -3
Console#
```

transceiver-threshold temperature This command sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold temperature {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high temperature threshold for an alarm message.

high-warning – Sets the high temperature threshold for a warning message.

low-alarm – Sets the low temperature threshold for an alarm message.

low-warning – Sets the low temperature threshold for a warning message.

threshold-value – The threshold of the transceiver temperature.
(Range: -12800 - 12800 in units of 0.01 Celsius)

Default Setting

High Alarm: 75.00 °C

High Warning: 70.00 °C

Low Alarm: -123.00 °C

Low Warning: 0.00 °C

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver temperature at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold temperature low-alarm 97
Console(config-if)#transceiver-threshold temperature high-alarm -83
Console#
```

transceiver-threshold tx-power This command sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold tx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the transmitted signal.
(Range: -4000 - 820 in units of 0.01 dBm)

Default Setting

High Alarm: -9.00 dBm
High Warning: -9.50 dBm
Low Warning: -11.50 dBm
Low Alarm: -12.00 dBm

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.

- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the signal power transmitted at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold tx-power low-alarm 8
Console(config-if)#transceiver-threshold tx-power high-alarm -3
Console#
```

transceiver-threshold voltage This command sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold voltage {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high voltage threshold for an alarm message.

high-warning – Sets the high voltage threshold for a warning message.

low-alarm – Sets the low voltage threshold for an alarm message.

low-warning – Sets the low voltage threshold for a warning message.

threshold-value – The threshold of the transceiver voltage.

(Range: 0-655 in units of 0.01 Volt)

Default Setting

High Alarm: 3.50 Volts

High Warning: 3.45 Volts

Low Warning: 3.15 Volts

Low Alarm: 3.10 Volts

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver voltage at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold voltage low-alarm 4
Console(config-if)#transceiver-threshold voltage high-alarm 2
Console#
```

show interfaces transceiver

This command displays identifying information for the specified transceiver, including connector type and vendor-related parameters, as well as the temperature, voltage, bias current, transmit power, and receive power.

Syntax

show interfaces transceiver [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-26/49-52)

Default Setting

Shows all SFP interfaces.

Command Mode

Privileged Exec

Command Usage

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, and received optical power, and related alarm thresholds.

Example

```
Console#show interfaces transceiver ethernet 1/28
Information of Eth 1/49
Connector Type       : LC
Fiber Type           : [0x00]
Eth Compliance Codes : 1000BASE-ZX
Baud Rate             : 1300 MBd
Vendor OUI           : 00-00-5F
Vendor Name          : SumitomoElectric
Vendor PN            : SCP6G94-FN-BWH
Vendor Rev           : Z
Vendor SN            : SE08T712Z00006
Date Code            : 10-09-14
```

```

DDM Info
  Temperature      : 35.64 degree C
  Vcc              : 3.25 V
  Bias Current     : 12.13 mA
  TX Power         : 2.36 dBm
  RX Power         : -24.20 dBm
DDM Thresholds
-----
          Low Alarm  Low Warning  High Warning  High Alarm
-----
Temperature(Celsius) -45.00      -40.00      85.00      90.00
Voltage(Volts)       2.90        3.00        3.60        3.70
Current(mA)          1.00        3.00       50.00       60.00
TxPower(dBm)        -11.50      -10.50       -2.00       -1.00
RxPower(dBm)        -23.98      -23.01       -1.00        0.00
Console#

```

show interfaces transceiver-threshold This command Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power. Syntax

Syntax

show interfaces transceiver-threshold [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-26/49-52)

Default Setting

Shows all SFP interfaces.

Command Mode

Privileged Exec

Command Usage

- ◆ The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, received optical power, and related alarm thresholds.
- ◆ The DDM thresholds displayed by this command only apply to ports which have a DDM-compliant transceiver inserted.

Example

```

Console#show interfaces transceiver-threshold ethernet 1/25
Information of Eth 1/25
DDM Thresholds
Transceiver-monitor      : Disabled
Transceiver-threshold-auto : Enabled

```

-----	Low Alarm	Low Warning	High Warning	High Alarm
-----	-----	-----	-----	-----
Temperature (Celsius)	-123.00	0.00	70.00	75.00
Voltage (Volts)	3.10	3.15	3.45	3.50
Current (mA)	6.00	7.00	90.00	100.00
TxPower (dBm)	-12.00	-11.50	-9.50	-9.00
RxPower (dBm)	-21.50	-21.00	-3.50	-3.00
Console#				

Cable Diagnostics

test cable-diagnostics This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

Syntax

test cable-diagnostics interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-22/48)

Command Mode

Privileged Exec

Command Usage

- ◆ Cable diagnostics are performed using an internal Digital Signal Processing test process when the port link-up speed is 1 Gbps. The method analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse. If the port link-up speed is not 1 Gbps, then Time Domain Reflectometry (TDR) test method is used. TDR also detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. However, note that TDR can only determine if a link is valid or faulty.
- ◆ This cable test is only accurate for Ethernet cables 7 - 100 meters long.
- ◆ The test takes approximately 5 seconds. Use the [show cable-diagnostics](#) command to display the results of the test, including common cable failures, as well as the status and approximate length of each cable pair.
- ◆ Ports are linked down while running cable diagnostics.
- ◆ To ensure more accurate measurement of the length to a fault, first disable power-saving mode (using the [no power-save](#) command) on the link partner before running cable diagnostics.

Example

```
Console#test cable-diagnostics interface ethernet 1/24
Console#
```

show cable-diagnostics This command shows the results of a cable diagnostics test.

Syntax

show cable-diagnostics interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-22/48)

Command Mode

Privileged Exec

Command Usage

- ◆ The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- ◆ For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.
- ◆ Potential conditions which may be listed by the diagnostics are shown by the legend in the following example. Additional information is provided for the following test results.
 - OK: Correctly terminated pair
 - ON: Open pair, no link partner
 - IE (Impedance mismatch): Terminating impedance is not in the reference range.
 - NS (Not Supported): This message is displayed for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
 - UN: Unknown Error

Example

```
Console#show cable-diagnostics interface ethernet 1/24
Cable Diagnostics on interface Ethernet 1/1:
Cable Open with accuracy 0 meters.
  Pair A Open, length 2 meters
  Pair B Open, length 2 meters
  Pair C Short, length 0 meters
  Pair D Short, length 0 meters
  Last Update On 2011-02-16 02:32:56
Console#
```


Power Savings

power-save This command enables power savings mode on the specified port. Use the **no** form to disable this feature.

Syntax

[no] power-save

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet ports 1-22/48)

Command Usage

- ◆ Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- ◆ Power savings can be enabled on Gigabit Ethernet RJ-45 ports.
- ◆ The power-saving methods provided by this switch include:
 - Power saving when there is no link partner:

Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.
 - Power saving when there is a link partner:

Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When power-savings mode is enabled, the switch determines whether or not it can reduce the signal amplitude used on a particular link.
- ◆ When the power-save command is enabled and traffic is reduced there is a reduction in power. For example, factory hardware component testing has shown significant power reduction >10%-45%⁹ are realized when 1000M Ethernet ports operate at slower rates from 300 to 0 Mbps.

9. The percentage reduction is for the switch hardware interface internal component only.



Note: Power savings can only be implemented on Gigabit Ethernet ports using twisted-pair cabling. Power-savings mode on a active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

Example

```
Console(config)#interface ethernet 1/24
Console(config-if)#power-save
Console(config-if)#
```

show power-save This command shows the configuration settings for power savings.

Syntax

show power-save [**interface** *interface*]
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-22/48)

Command Mode

Privileged Exec

Example

```
Console#show power-save interface ethernet 1/24
Power Saving Status:
 Ethernet 1/24 : Enabled
Console#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 8 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 72: Link Aggregation Commands

Command	Function	Mode
<i>Manual Configuration Commands</i>		
<code>interface port-channel</code>	Configures a trunk and enters interface configuration mode for the trunk	GC
<code>port channel load-balance</code>	Sets the load-distribution method among ports in aggregated links	GC
<code>channel-group</code>	Adds a port to a trunk	IC (Ethernet)
<i>Dynamic Configuration Commands</i>		
<code>lacp</code>	Configures LACP for the current interface	IC (Ethernet)
<code>lacp admin-key</code>	Configures a port's administration key	IC (Ethernet)
<code>lacp port-priority</code>	Configures a port's LACP port priority	IC (Ethernet)
<code>lacp system-priority</code>	Configures a port's LACP system priority	IC (Ethernet)
<code>lacp admin-key</code>	Configures an port channel's administration key	IC (Port Channel)
<code>lacp timeout</code>	Configures the timeout to wait for next LACPDU	IC (Port Channel)
<i>Trunk Status Display Commands</i>		
<code>show interfaces brief</code>	Shows static and dynamic trunk information	NE, PE
<code>show interfaces status port-channel</code>	Shows static and dynamic trunk information	NE, PE
<code>show lacp</code>	Shows LACP information	PE
<code>show port-channel load-balance</code>	Shows the load-distribution method used on aggregated links	PE

Guidelines for Creating Trunks

General Guidelines –

- ◆ Finish configuring trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- ◆ A trunk can have up to 8 ports.
- ◆ The ports at both ends of a connection must be configured as trunk ports.
- ◆ All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- ◆ Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- ◆ All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- ◆ STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- ◆ Ports must have the same LACP system priority.
- ◆ Ports must have the same port admin key (Ethernet Interface).
- ◆ If the port channel admin key ([lACP admin key](#) - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key ([lACP admin key](#) - Ethernet Interface) used by the interfaces that joined the group.
- ◆ However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- ◆ If a link goes down, LACP port priority is used to select the backup link.

Manual Configuration Commands

port channel load-balance This command sets the load-distribution method among ports in aggregated links (for both static and dynamic trunks). Use the **no** form to restore the default setting.

Syntax

port channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port channel load-balance

dst-ip - Load balancing based on destination IP address.

dst-mac - Load balancing based on destination MAC address.

src-dst-ip - Load balancing based on source and destination IP address.

src-dst-mac - Load balancing based on source and destination MAC address.

src-ip - Load balancing based on source IP address.

src-mac - Load balancing based on source MAC address.

Default Setting

src-dst-ip

Command Mode

Global Configuration

Command Usage

- ◆ This command applies to all static and dynamic trunks on the switch.
- ◆ To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:
 - **dst-ip:** All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
 - **dst-mac:** All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
 - **src-dst-ip:** All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.
 - **src-dst-mac:** All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.
 - **src-ip:** All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.

- **src-mac:** All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

Example

```
Console(config)#port channel load-balance dst-ip
Console(config)#
```

channel-group This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*

no channel-group

channel-id - Trunk index (Range: 1-8)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- ◆ Use **no channel-group** to remove a port group from a trunk.
- ◆ Use **no interface port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 10:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#
```

Dynamic Configuration Commands

lacp This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[no] lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- ◆ A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- ◆ If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- ◆ If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 1-3. Because LACP has also been enabled on the ports at the other end of the links, the [show interfaces status port-channel 1](#) command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/2
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/3
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic Information:
  Port Type           : 1000BASE-T
  MAC Address         : 12-34-12-34-12-3F
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : Auto
  Capabilities        : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 500 packets/second
```

```
Multicast Storm          : Disabled
Multicast Storm Limit    : 500 packets/second
Unknown Unicast Storm    : Disabled
Unknown Unicast Storm Limit : 500 packets/second
Storm Threshold Resolution : 1 packets/second
Flow Control             : Disabled
MAC Learning             : Enabled
Link-up-down Trap        : Enabled
Current status:
Created By               : LACP
Link Status              : Up
Port Operation Status    : Up
Operation Speed-duplex   : 1000full
Up Time                  : 0w 0d 0h 0m 53s (53 seconds)
Flow Control Type        : None
Max Frame Size           : 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status      : Enabled
Member Ports             : Eth1/1, Eth1/2, Eth1/3,
Active Member Ports      : Eth1/1, Eth1/2, Eth1/3,
Console#
```

lacp admin-key (Ethernet Interface) This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} admin-key key

no lacp {actor | partner} admin-key

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

key - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

Actor: 1, Partner: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- ◆ If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.

- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.



Note: Configuring the partner admin-key does not affect remote or local switch operation. The local switch just records the partner admin-key for user reference.

- ◆ By default, the actor's operational key is determined by port's link speed (1000f - 4, 100f - 3, 10f - 2), and copied to the admin key.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp port-priority This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} port-priority *priority*

no lacp {actor | partner} port-priority

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Setting a lower value indicates a higher effective priority.
- ◆ If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- ◆ If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5  
Console(config-if)#lacp actor port-priority 128
```

lacp system-priority This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} system-priority *priority*

no lacp {actor | partner} system-priority

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Port must be configured with the same system priority to join the same LAG.
- ◆ System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5  
Console(config-if)#lacp actor system-priority 3  
Console(config-if)#
```

lacp admin-key (Port Channel) This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*

no lacp admin-key

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch.
(Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- ◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- ◆ If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.
- ◆ If the port channel admin key is set to a non-default value, the operational key is based upon LACP PDUs received from the partner, and the channel admin key is reset to the default value. The trunk identifier will also be changed by this process.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp timeout This command configures the timeout to wait for the next LACP data unit (LACPDU). Use the no form to restore the default setting.

Syntax

lacp timeout {long | short}

no lacp timeout

long - Specifies a slow timeout of 90 seconds.

short - Specifies a fast timeout of 3 seconds.

Default Setting

long

Command Mode

Interface Configuration (Port Channel)

Command Usage

- ◆ The timeout configured by this command is set in the LACP timeout bit of the Actor State field in transmitted LACPDU. When the partner switch receives an LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds.
- ◆ If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group.
- ◆ When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port.
- ◆ When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp timeout short
Console(config-if)#
```

Trunk Status Display Commands

show lacp This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sysid**}

port-channel - Local identifier for a link aggregation group. (Range: 1-8)

counters - Statistics for LACP protocol messages.

internal - Configuration settings and operational state for local side.

neighbors - Configuration settings and operational state for remote side.

sysid - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Port Channel: 1
Member Port           : Eth 1/24
LACPDU Sent           : 7
LACPDU Received       : 6
MarkerPDU Sent        : 0
MarkerPDU Received    : 0
MarkerResponsePDU Sent : 0
MarkerResponsePDU Received : 0
Unknown Packet Received : 0
Illegal Packet Received : 0
:
```

Table 73: show lacp counters - display description

Field	Description
LACPDU Sent	Number of valid LACPDU transmitted from this channel group.
LACPDU Received	Number of valid LACPDU received on this channel group.
Marker Sent	Number of valid Marker PDU transmitted from this channel group.
Marker Received	Number of valid Marker PDU received by this channel group.
MarkerResponsePDU Sent	Number of valid MarkerResponse PDU transmitted from this channel group.
MarkerResponsePDU Received	Number of valid MarkerResponse PDU received by this channel group.

Table 73: show lacp counters - display description (Continued)

Field	Description
Unknown Packet Received	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Unknown Packet Received	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```

Console#show lacp 1 internal
Vty-1#show lacp 1 internal
Port Channel : 1
Admin Key    : 1
Oper Key     : 1
Timeout      : Long
-----
Member Port   : Eth 1/15
Periodic Time : 30 seconds
System Priority : 32768
Port Priority  : 32768
Admin Key     : 1
Oper Key      : 1
Admin State   : Defaulted, Aggregatable, Long Timeout, Passive LACP
Oper State    : Distributing, Collecting, Synchronization, Aggregatable,
                  Long Timeout, Passive LACP
:

```

Table 74: show lacp internal - display description

Field	Description
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.
Timeout	Time to wait for the next LACPDU before deleting partner port information.
Periodic Time	Number of seconds before invalidating received LACPDU information.
System Priority	LACP system priority assigned to this port channel.
Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: <ul style="list-style-type: none"> Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.

Table 74: show lacp internal - display description (Continued)

Field	Description
Admin State, Oper State (continued)	<ul style="list-style-type: none"> ♦ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. ♦ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. ♦ LACP Active or LACP Passive - The configured LACP mode.

```

Console#show lacp 1 neighbors
Port Channel : 1
-----

Member Port           : Eth 1/15
Partner Admin System ID : 32768, 00-00-00-00-00-00
Partner Oper System ID  : 32768, 70-72-CF-92-9A-71
Partner Admin Port ID   : 32768, 15
Partner Oper Port ID    : 32768, 15
Partner Admin Key       : 1
Partner Oper Key        : 1
Partner Admin State     : Defaulted, Distributing, Collecting,
                        Synchronization, Long Timeout, Passive LACP
Partner Oper State      : Distributing, Collecting, Synchronization,
                        Aggregatable, Long Timeout, Active LACP
:

```

Table 75: show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port ID	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```

Console#show lacp sysid
Port Channel    System Priority    System MAC Address
-----
1               32768             00-30-F1-8F-2C-A7
2               32768             00-30-F1-8F-2C-A7
3               32768             00-30-F1-8F-2C-A7

```

```
4          32768      00-30-F1-8F-2C-A7
5          32768      00-30-F1-8F-2C-A7
6          32768      00-30-F1-8F-2C-A7
7          32768      00-30-F1-D4-73-A0
8          32768      00-30-F1-D4-73-A0
9          32768      00-30-F1-D4-73-A0
10         32768      00-30-F1-D4-73-A0
11         32768      00-30-F1-D4-73-A0
12         32768      00-30-F1-D4-73-A0
:
```

Table 76: show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

show port-channel load-balance This command shows the load-distribution method used on aggregated links.

Command Mode

Privileged Exec

Example

```
Console#show port-channel load-balance
Trunk Load Balance Mode: Destination IP address
Console#
```


Power over Ethernet Commands

For switches that support PoE power, the commands in this group control the power that can be delivered to attached PoE devices through RJ-45 ports.

The switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Table 77: PoE Commands

Command	Function	Mode
<code>power inline compatible</code>	Provides power to pre-standard PoE devices	GC
<code>power inline maximum allocation mode</code>	Sets the maximum power allocation mode based on PD class or user configuration	GC
<code>power mainpower maximum allocation</code>	Sets the maximum power available to all switch ports	GC
<code>power inline</code>	Sets the port to detect if a PoE compatible device is connected and turn on or off power.	IC
<code>power inline maximum allocation</code>	Sets the maximum power available to specific switch ports	IC
<code>power inline priority</code>	Sets the priority for power supplied to specific ports	IC
<code>power inline time-range</code>	Binds a time-range to a port during which PoE is supplied	IC
<code>show power inline status</code>	Displays the current status of power management on specific ports or all ports	PE
<code>show power mainpower</code>	Displays the current status of power management for switch	PE
<code>show power inline time-range</code>	Shows the time-range and current status for specific ports or for all ports	PE

power inline compatible This command allows the switch to detect and provide power to powered devices that were designed prior to the IEEE 802.3af PoE standard. Use the **no** form to disable this feature.

Syntax

[no] power inline compatible *unit*

unit - Unit identifier. (Range: 1)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The switch automatically detects attached PoE devices by periodically transmitting test voltages that over the Gigabit Ethernet copper-media ports. When an IEEE 802.3af or 802.3at compatible device is plugged into one of these ports, the powered device reflects the test voltage back to the switch, which may then turn on the power to this device. When the **power inline compatible** command is used, this switch can detect IEEE 802.3af or 802.3at compliant devices and the more recent 802.3af non-compliant devices that also reflect the test voltages back to the switch. It cannot detect other legacy devices that do not reflect back the test voltages.
- ◆ For legacy devices to be supported by this switch, they must be able to accept power over the data pairs connected to the RJ-45 ports.

Example

```
Console(config)#power inline compatible
Console(config)#
```

**power inline
maximum allocation
mode**

This command sets the maximum power allocation mode based on PD (powered device) class or user configuration. Use the **no** form to restore the default setting.

Syntax

power inline maximum allocation mode {class | user} unit

no power inline maximum allocation mode unit

class - Power allocation is based on device classification.

user - Power allocation is based on user configuration as defined in the [power mainpower maximum allocation](#) Global Configuration command or the [power inline maximum allocation](#) Interface Configuration command.

unit - Unit identifier. (Range: 1)

Default Setting

class

Command Mode

Global Configuration

Command Usage

The IEEE standard does not define the maximum power of each PD class. The following table is an example from Microsem's PoE IC implementation.

Table 78: Maximum PoE Based on PD Classification

PD Class	Maximum Power (Watts)
Class 0 (AF)	16.1
Class 0 (AT)	33.6
Class 1	4.2
Class 2	7.3
Class 3	16.1
Class 4	33.6

Example

```
Console(config)#power inline maximum allocation mode user unit 1
Console(config)#
```

power mainpower maximum allocation

This command defines a power budget for the switch (i.e., the power available to all switch ports). Use the **no** form to restore the default setting.

Syntax

power mainpower maximum allocation *milliwatts unit*

no power mainpower maximum allocation *unit*

milliwatts - The power budget for the switch. (Range: 50000-125000 mW)

unit - Unit identifier. (Range: 1)

Default Setting

125000 mW

Command Mode

Global Configuration

Command Usage

- ◆ Setting a maximum power budget for the switch enables power to be centrally managed, preventing overload conditions at the power source.
- ◆ If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.

Example

```
Console(config)#power mainpower maximum allocation 180000 unit 1
Console(config)#
```

Related Commands

[power inline priority \(397\)](#)

power inline This command instructs the switch to automatically detect if a PoE-compliant device is connected to the specified port, and turn power on or off accordingly. Use the **no** form to turn off power for a port.

Syntax

power inline

no power inline

Default Setting

Detection is enabled for PoE-compliant devices.

Command Mode

Interface Configuration (Ethernet ports 1-8/24)

Command Usage

- ◆ The switch only provides power to the Gigabit Ethernet RJ-45 ports.
- ◆ When detection is enabled for PoE-compliant devices, power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed the port's power budget or the switch's power budget.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#no power inline
Console(config-if)#
```

power inline maximum allocation This command limits the power allocated to specific ports. Use the **no** form to restore the default setting.

Syntax

power inline maximum allocation *milliwatts*

no power inline maximum allocation

milliwatts - The maximum power budget for the port.
(Range: 3000-34200 milliwatts)

Default Setting

34200 milliwatts

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The number of ports which can supply maximum power simultaneously to connected devices is listed in the following table.

Table 79: Maximum Number of Ports Providing Simultaneous Power

Switch	30W (802.3at)	15.4W (802.3af)	7.5W (802.3af)
GEL-1061	4	8	8

- ◆ If a device is connected to a switch port and the switch detects that it requires more than the maximum power allocated to the port or to the overall switch, no power is supplied to the device (i.e., port power remains off).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline maximum allocation 8000
Console(config-if)#
```

power inline priority This command sets the power priority for specific ports. Use the **no** form to restore the default setting.

Syntax

power inline priority *priority*

no power inline priority

priority - The power priority for the port.
Options: 1 (critical), 2 (high), or 3 (low)

Default Setting

3 (low)

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Port priority determines which port will have power turned off first when the switch power budget is exceeded.

- ◆ If the priority of two ports is the same, the port with the lowest port number will have the higher priority. For example, if all port priorities are set to low, the priority order will become port 1 > port 2 > port 3 > port 4 > port 5 > port 6 and so on.
- ◆ If the power demand from devices connected to the switch exceeds the power budget setting as determined during bootup, the switch uses port power priority settings to control the supplied power in the following ways:
 - A device connected to a low-priority port that causes the switch to exceed its budget will not be supplied power.
 - A device may be connected to a critical or high priority port. If during switch bootup, this device causes the switch to exceed its power budget; the switch will determine if it can supply power to the port or not. Power is only provided to the port if the switch can drop power to one or more lower-priority ports and remain within its configured power budget. Power will be dropped from lower-priority ports starting in reverse sequence from the highest PoE enabled port number.
 - If sufficient power cannot be made available by turning off power to lower-priority ports, power may not be supplied to a device connected to a high or critical priority port.
- ◆ The priority setting will be ignored if a device is connected to a port after the switch has finished booting up. When a newly connected device causes the switch to exceed its budget, power will not be provided to that device's port regardless of its priority setting.
 - If priority is not set for any ports, and PoE consumption exceeds the maximum power provided by the switch, power is shut down in reverse sequence from port number.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline priority 2
Console(config-if)#
```

power inline time-range This command binds a time-range to a port during which PoE is supplied to the attached device. Use the **no** form to remove this binding.

Syntax

power inline time-range *time-range-name*
no power inline time-range

time-range-name - Name of the time range. (Range: 1-32 characters)

Default Setting

None

Command Mode

Interface Configuration

Example

```

Console(config)#interface ethernet 1/1
Console(config-if)#power inline time-range rd
Console(config-if)#

```

Related Commands[time-range \(149\)](#)

show power inline status This command displays the current power status for all ports or for specific ports.

Syntax**show power inline status** [*interface*]*interface***ethernet***unit* - Unit identifier. (Range: 1)*port* - Port number. (Ethernet ports 1-8/24)**Command Mode**

Privileged Exec

Example

```

Console#show power inline status
Unit: 1
Compatible Mode : Disabled
Maximum Allocation Mode : User mode

```

Interface	Admin	Time Range	Oper Class	Max Power	Used Power	Priority
Eth 1/ 1	Enabled	--	Off	- 3360 mW	0 mW	Low
Eth 1/ 2	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 3	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 4	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 5	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 6	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 7	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 8	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/ 9	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/10	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/11	Enabled	--	Off	- 33600 mW	0 mW	Low
Eth 1/12	Enabled	--	Off	- 33600 mW	0 mW	Low
.						

Table 80: show power inline status - display description

Field	Description
Compatible Mode	Shows if the switch detects and provides power to powered devices that were designed prior to the IEEE 802.3af PoE standard (see power inline compatible)
Maximum Allocation Mode	The maximum power allocation mode based on the global configuration command power mainpower maximum allocation
Interface	The PoE port
Admin	The administrative power mode set on the port (see power inline)
Time Range	The time range during which power is supplied (see time-range)
Oper	The current operating power status (displays on or off). Note that if power is turned off due to an overload, administrative status will still display enabled.
Class	Shows the maximum power allocation class if defined by the global configuration command power mainpower maximum allocation . Class information is shown only when Oper = On.
Max Power	The maximum power allocated to this port (see power inline maximum allocation)
Used Power	The current power consumption on the port in milliwatts
Priority	The port's power priority setting (see power inline priority)

show power inline time-range This command displays the time-range and current status for specific ports or for all ports.

Syntax

show power inline time-range *time-range-name* [*interface*]

time-range-name - Name of the time range. (Range: 1-32 characters)

interface

ethernet

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-8/24)

Command Mode

Privileged Exec

Example

```

Console#show power inline time-range ethernet 1/5
Interface Time Range Name  Status
-----
Eth 1/ 5   r&d             Inactive
Console#

```

Related Commands

[power inline \(396\)](#)

show power mainpower Use this command to display the current power status for the switch.

Syntax

show power mainpower *unit*

unit - Unit identifier. (Range: 1)

Command Mode

Privileged Exec

Example

This example shows the maximum available PoE power and maximum allocated PoE power.

```
Console#show power mainpower unit 1
Unit 1 PoE Status
PoE Maximum Available Power : 200.0 Watts (using internal power)
PoE Maximum Allocation Power : 50.0 Watts
System Operation Status      : On
PoE Power Consumption        : 15.2 Watts
Software Version              : Version 00A1 (Hex), Build 09 (Hex)
```

```
Console#
```

Table 81: show power mainpower - display description

Field	Description
PoE Maximum Available Power	The available power budget for the switch
PoE Maximum Allocation Power	The power budget for the switch. If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power.
System Operation Status	The current operating power status (displays on or off)
PoE Power Consumption	The current power consumption on the switch in watts
Software Version	The version of software running on the PoE controller subsystem in the switch.

Port Mirroring Commands

Data can be mirrored from a local port on the same switch or from a remote port on another switch for analysis at the target port using software monitoring tools or a hardware probe. This switch supports the following mirroring modes.

Table 82: Port Mirroring Commands

Command	Function
Local Port Mirroring	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
RSPAN Mirroring	Mirrors data from remote switches over a dedicated VLAN

Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

Table 83: Mirror Port Commands

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

port monitor This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]

no port monitor *interface*

interface

ethernet *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

- ◆ No mirror session is defined.
- ◆ When enabled for an interface, default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- ◆ You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- ◆ Set the destination port by specifying an Ethernet interface with the [interface](#) configuration command, and then use the [port monitor](#) command to specify the source of the traffic to mirror. Note that the destination port cannot be a trunk or trunk member port.
- ◆ When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- ◆ Spanning Tree BPDU packets are not mirrored to the target port.
- ◆ You can create multiple mirror sessions, but all sessions must share the same destination port.
- ◆ The destination port cannot be a trunk or trunk member port.

Example

The following example configures the switch to mirror all packets from port 6 to 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination Port (listen port) : Eth 1/12
Source Port (monitored Port)  : Eth 1/ 1
Mode                          : RX/TX
Console#
```

RSPAN Mirroring Commands

Remote Switched Port Analyzer (RSPAN) allows you to mirror traffic from remote switches for analysis on a local destination port.

Table 84: RSPAN Commands

Command	Function	Mode
<code>vlan rspan</code>	Creates a VLAN dedicated to carrying RSPAN traffic	VC
<code>rspan source</code>	Specifies the source port and traffic type to be mirrored	GC
<code>rspan destination</code>	Specifies the destination port to monitor the mirrored traffic	GC
<code>rspan remote vlan</code>	Specifies the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports	GC
<code>no rspan session</code>	Deletes a configured RSPAN session	GC
<code>show rspan</code>	Displays the configuration settings for an RSPAN session	PE

Configuration Guidelines

Take the following steps to configure an RSPAN session:

1. Use the [vlan rspan](#) command to configure a VLAN to use for RSPAN. (Default VLAN 1 is prohibited.)
2. Use the [rspan source](#) command to specify the interfaces and the traffic type (RX, TX or both) to be monitored.
3. Use the [rspan destination](#) command to specify the destination port for the traffic mirrored by an RSPAN session.
4. Use the [rspan remote vlan](#) command to specify the VLAN to be used for an RSPAN session, to specify the switch's role as a source, intermediate relay, or destination of the mirrored traffic, and to configure the uplink ports designated to carry this traffic.

RSPAN Limitations

The following limitations apply to the use of RSPAN on this switch:

- ◆ *RSPAN Ports* – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.

Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink or destination port – access ports are not allowed (see [switchport mode](#)).

- ◆ *Local/Remote Mirror* – The destination of a local mirror session (created with the [port monitor](#) command) cannot be used as the destination for RSPAN traffic.
- ◆ *Spanning Tree* – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.

MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.

- ◆ *IEEE 802.1X* – RSPAN and 802.1X are mutually exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

RSPAN uplink ports cannot be configured to use IEEE 802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it

- ◆ *Port Security* – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

rspan source Use this command to specify the source port and traffic type to be mirrored remotely. Use the **no** form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

Syntax

[no] rspan session session-id source interface interface-list [rx | tx | both]

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

interface-list – One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

Default Setting

Both TX and RX traffic is mirrored

Command Mode

Global Configuration

Command Usage

- ◆ One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
- ◆ Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.
- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN source port – access ports are not allowed (see [switchport mode](#)).
- ◆ The source port and destination port cannot be configured on the same switch.

Example

The following example configures the switch to mirror received packets from port 2 and 3:

```
Console(config)#rspan session 1 source interface ethernet 1/2
Console(config)#rspan session 1 source interface ethernet 1/3
Console(config)#
```

rspan destination Use this command to specify the destination port to monitor the mirrored traffic. Use the **no** form to disable RSPAN on the specified port.

Syntax

rspan session *session-id* **destination interface** *interface* [**tagged** | **untagged**]

no rspan session *session-id* **destination interface** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

tagged - Traffic exiting the destination port carries the RSPAN VLAN tag.

untagged - Traffic exiting the destination port is untagged.

Default Setting

Traffic exiting the destination port is untagged.

Command Mode

Global Configuration

Command Usage

- ◆ Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.
- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN destination port – access ports are not allowed (see [switchport mode](#)).
- ◆ Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.
- ◆ The source port and destination port cannot be configured on the same switch.

- ◆ A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

Example

The following example configures port 4 to receive mirrored RSPAN traffic:

```
Console(config)#rspan session 1 destination interface ethernet 1/2
Console(config)#
```

rspan remote vlan Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the **no** form to disable the RSPAN on the specified VLAN.

Syntax

[no] rspan session *session-id* **remote vlan** *vlan-id*
{source | intermediate | destination} **uplink** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

vlan-id - ID of configured RSPAN VLAN. (Range: 1-4094)

Use the **vlan rspan** command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

source - Specifies this device as the source of remotely mirrored traffic.

intermediate - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

destination - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

uplink - A port configured to receive or transmit remotely mirrored traffic.

interface - **ethernet** *unit/port*

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink port – access ports are not allowed (see [switchport mode](#)).
- ◆ Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.
- ◆ Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the [switchport allowed vlan](#) command. Also, note that the [show vlan](#) command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

Example

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

no rspan session Use this command to delete a configured RSPAN session.

Syntax

no rspan session *session-id*

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

Command Mode

Global Configuration

Command Usage

The **no rspan session** command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the [vlan](#) command).

Example

```
Console(config)#no rspan session 1
Console(config)#
```

show rspan Use this command to displays the configuration settings for an RSPAN session.

Syntax

show rspan session [*session-id*]

session-id – A number identifying this RSPAN session. (Range: 1)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

Command Mode

Privileged Exec

Example

```
Console#show rspan session
RSPAN Session ID           : 1
Source Ports (mirrored ports) : None
  RX Only                   : None
  TX Only                   : None
  BOTH                      : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode      : Untagged
Switch Role                  : Destination
RSPAN VLAN                   : 2
RSPAN Uplink Ports           : Eth 1/3
Operation Status              : Up
Console#
```


Congestion Control Commands

The switch can set the maximum upload or download data transfer rate for any port. It can control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Table 85: Congestion Control Commands

Command Group	Function
Rate Limiting	Sets the input and output rate limits for a port.
Storm Control	Sets the traffic storm threshold for each port.

Rate Limit Commands

Rate limit commands allow the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 86: Rate Limit Commands

Command	Function	Mode
rate-limit	Configures the maximum input or output rate for an interface	IC

rate-limit This command defines the rate limit for a specific interface. Use this command without specifying a rate to enable rate limiting. Use the **no** form to disable rate limiting.

Syntax

rate-limit {input | output} [*rate*]

no rate-limit {input | output}

input – Input rate for specified interface

output – Output rate for specified interface

rate – Maximum value in kbps.

(Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports;

64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)

The resolution at which the rate can be configured is 16 kbits/sec.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.
- ◆ Using the no form of the command will disable rate-limiting on the interface. When the command [show interfaces switchport](#) is executed, the parameters "Ingress Rate Limit" and "Egress Rate Limit" will be shown as disabled and the full port speed will be displayed. Refer to the command example where rate limit for the output is disabled.
- ◆ When a rate-limit is applied, the command will be shown in the running-config file. However, when the no form of the command is entered, the original rate-limit command will remain in the running-config file with the additional no form of the command immediately below. Refer to the console output below:

```
Console#config
Console(config)#interface ethernet 1/4
Console(config-if)#rate-limit output 200
Console(config-if)#end
Console#show running-config
~
interface ethernet 1/3

!
interface ethernet 1/4
  rate-limit output 200

!
interface ethernet 1/5
```

```

~
Console#config
Console(config)#interface ethernet 1/4
Console(config-if)#no rate-limit output
Console(config-if)#end
Console#show running-config
~
interface ethernet 1/3

!
interface ethernet 1/4
  rate-limit output 200
  no rate-limit output

!
interface ethernet 1/5
~

```

- ◆ If the no form of the command accompanies the rate-limit in the running-config file, the rate-limiting function is disabled.
- ◆ To remove the rate-limit from the running-config file. Use the following procedure:
 - 1. Set the rate limit to the maximum for the port e.g. **rate-limit input 1000000**.
 - 2. Enter the no form of the command e.g. **no rate-limit input**.

Example

In this example Ethernet port 1's Ingress (input) Rate Limit is restricted to 64 kbits/second and the port's Egress (output) Rate Limit is disabled.

```

Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#no rate-limit output
Console(config-if)#end
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
Broadcast Threshold           : Disabled
Multicast Threshold           : Disabled
Unknown Unicast Threshold     : Disabled
Storm Threshold Resolution    : 1 packets/second
LACP Status                   : Disabled
Ingress Rate Limit            : Enabled, 64 kbits/second
Egress Rate Limit             : Disabled, 1000000 kbits/second
Rate Limit Resolution         : 16 kbits/second
VLAN Membership Mode          : Hybrid
Ingress Rule                  : Enabled
Acceptable Frame Type         : All frames
Native VLAN                   : 1
Priority for Untagged Traffic  : 0
Allowed VLAN                   :      1(u)
Forbidden VLAN                 :
802.1Q Tunnel Status          : Disabled
802.1Q Tunnel Mode            : Normal

```

```
802.1Q Tunnel TPID          : 8100 (Hex)
Console#
```

Related Command

[show interfaces switchport \(365\)](#)

Storm Control Commands

Storm control commands can be used to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Table 87: Rate Limit Commands

Command	Function	Mode
switchport packet-rate	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE

switchport packet-rate This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

Syntax

switchport {broadcast | multicast | unknown-unicast} packet-rate *rate*

no switchport {broadcast | multicast | unknown-unicast}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unknown-unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level as a rate; i.e. (Range: 500-262142 pps)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

Related Commands

[show interfaces switchport \(365\)](#)

Loopback Detection Commands

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Table 88: Loopback Detection Commands

Command	Function	Mode
<code>loopback-detection</code>	Enables loopback detection globally on the switch or on a specified interface	GC, IC
<code>loopback-detection action</code>	Specifies the response to take for a detected loopback condition	GC
<code>loopback-detection recover-time</code>	Specifies the interval to wait before releasing an interface from shutdown state	GC
<code>loopback-detection transmit-interval</code>	Specifies the interval at which to transmit loopback detection control frames	GC
<code>loopback detection trap</code>	Configures the switch to send a trap when a loopback condition is detected or the switch recover from a loopback	GC
<code>loopback-detection release</code>	Manually releases all interfaces currently shut down by the loopback detection feature	PE
<code>show loopback-detection</code>	Shows loopback detection configuration settings for the switch or for a specified interface	PE

Usage Guidelines

- ◆ The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.
- ◆ General loopback detection provided by the commands described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.
- ◆ When a loopback event is detected on an interface or when a interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- ◆ Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

loopback-detection This command enables loopback detection globally on the switch or on a specified interface. Use the **no** form to disable loopback detection.

Syntax

[no] loopback-detection

Default Setting

Enabled

Command Mode

Global Configuration

Interface Configuration (Ethernet, Port Channel)

Command Usage

Loopback detection must be enabled globally for the switch by this command and enabled for a specific interface for this function to take effect.

Example

This example enables general loopback detection on the switch, disables loopback detection provided for the spanning tree protocol on port 1, and then enables general loopback detection for that port.

```
Console(config)#loopback-detection
Console(config)#interface ethernet 1/1
Console(config-if)#no spanning-tree loopback-detection
Console(config-if)#loopback-detection
Console(config)#
```

loopback-detection action This command specifies the protective action the switch takes when a loopback condition is detected. Use the **no** form to restore the default setting.

Syntax

loopback-detection action {none | shutdown}

no loopback-detection action

none - No action is taken.

shutdown - Shuts down the interface.

Default Setting

Shut down

Command Mode

Global Configuration

Command Usage

- ◆ When a port receives a control frame sent by itself, this means that the port is in looped state, and the VLAN in the frame payload is also in looped state with the wrong VLAN tag. The looped port is therefore shut down.
- ◆ Use the `loopback-detection recover-time` command to set the time to wait before re-enabling an interface shut down by the loopback detection process.
- ◆ When the loopback detection response is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

Example

This example sets the loopback detection mode to shut down user traffic.

```
Console(config)#loopback-detection action shutdown
Console(config)#
```

**loopback-detection
recover-time**

This command specifies the interval to wait before the switch automatically releases an interface from shutdown state. Use the **no** form to restore the default setting.

Syntax

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds - Recovery time from shutdown state. (Range: 60-1,000,000 seconds, or 0 to disable automatic recovery)

Default Setting

60 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.
- ◆ If the recovery time is set to zero, all ports placed in shutdown state can be restored to operation using the `loopback-detection release` command. To restore a specific port, use the `no shutdown` command.

Example

```
Console(config)#loopback-detection recover-time 120
Console(config-if)#
```

loopback-detection transmit-interval This command specifies the interval at which to transmit loopback detection control frames. Use the **no** form to restore the default setting.

Syntax

loopback-detection transmit-interval *seconds*

no loopback-detection transmit-interval

seconds - The transmission interval for loopback detection control frames.
(Range: 1-32767 seconds)

Default Setting

10 seconds

Command Mode

Global Configuration

Example

```
Console(config)#loopback-detection transmit-interval 60
Console(config)#
```

loopback detection trap This command sends a trap when a loopback condition is detected, or when the switch recovers from a loopback condition. Use the **no** form to restore the default state.

Syntax

loopback-detection trap [**both** | **detect** | **none** | **recover**]

no loopback-detection trap

both - Sends an SNMP trap message when a loopback condition is detected, or when the switch recovers from a loopback condition.

detect - Sends an SNMP trap message when a loopback condition is detected.

none - Does not send an SNMP trap for loopback detection or recovery.

recover - Sends an SNMP trap message when the switch recovers from a loopback condition.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Refer to the [loopback-detection recover-time](#) command for information on conditions which constitute loopback recovery.

Example

```
Console(config)#loopback-detection trap both
Console(config)#
```

loopback-detection release This command releases all interfaces currently shut down by the loopback detection feature.

Syntax**loopback-detection release****Command Mode**

Privileged Exec

Example

```
Console#loopback-detection release
Console(config)#
```

show loopback-detection This command shows loopback detection configuration settings for the switch or for a specified interface.

Syntax**show loopback-detection** [*interface*]*interface***ethernet** *unit/port**unit* - Unit identifier. (Range: 1)*port* - Port number. (Range: 1-10/28)**Command Mode**

Privileged Exec

Example

```
Console#show loopback-detection
Loopback Detection Global Information
Global Status      : Enabled
Transmit Interval : 10
```

```
Recover Time      : 60
Action            : Shutdown
Trap              : None
Loopback Detection Port Information
Port      Admin State Oper State
-----
Eth 1/ 1   Enabled    Normal
Eth 1/ 2   Disabled   Disabled
Eth 1/ 3   Disabled   Disabled
:
Console#show loopback-detection ethernet 1/1
Loopback Detection Information of Eth 1/1
Admin State : Enabled
Oper State  : Normal
Looped VLAN : None
Console#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 89: Address Table Commands

Command	Function	Mode
<code>mac-address-table aging-time</code>	Sets the aging time of the address table	GC
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>clear mac-address-table dynamic</code>	Removes any learned entries from the forwarding database	PE
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show mac-address-table aging-time</code>	Shows the aging time for the address table	PE
<code>show mac-address-table count</code>	Shows the number of MAC addresses used and the number of available MAC addresses	PE

mac-address-table aging-time This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 6-7200 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

mac-address-table static This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

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

mac-address - MAC address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- ◆ Static addresses will not be removed from the address table when a given interface link is down.
- ◆ Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- ◆ A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic This command removes any learned entries from the forwarding database as related to the option specified.

Syntax

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

address

mac-address - MAC hardware address

mask - Bits to match in the address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan

vlan-id - VLAN ID (Range: 1-4094)

all - all learned entries

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Even if a hash collision for a MAC address is resolved, entries in the MAC address table are not removed until this command is issued to reset the table, or the system is reset.

Example

```
Console#clear mac-address-table dynamic interface ethernet 1/5
Console#
```

show mac-address-table This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

sort - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
 - Learn - Dynamic address entries
 - Config - Static entry
 - Security - Port Security
- ◆ The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- ◆ The maximum number of address entries is 8K.

Example

```

Console#show mac-address-table
Interface MAC Address      VLAN Type      Life Time
-----
CPU       00-E0-00-00-00-01        1 CPU      Delete on Reset
Eth 1/ 1  00-E0-0C-10-90-09        1 Learn    Delete on Timeout
Eth 1/ 1  00-E0-29-94-34-64        1 Learn    Delete on Timeout
Console#

```

show mac-address-table aging-time This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
Aging Status : Enabled
Aging Time: 300 sec.
Console#
```

show mac-address-table count This command shows the number of MAC addresses used and the number of available MAC addresses for the overall system or for an interface.

Syntax

show mac-address-table count [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Eth 1/1
Total Address Count      :0
Static Address Count     :0
Dynamic Address Count    :0

Console#show mac-address-table count

Compute the number of MAC Address...

Maximum number of MAC Address which can be created in the system:
Total Number of MAC Address      : 16384
Number of Static MAC Address     : 1024
```

```
Current number of entries which have been created in the system:  
Total Number of MAC Address      : 3  
Number of Static MAC Address     : 1  
Number of Dynamic MAC Address    : 2  
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 90: Spanning Tree Commands

Command	Function	Mode
<code>spanning-tree</code>	Enables the spanning tree protocol	GC
<code>spanning-tree cisco-prestandard</code>	Configures spanning tree operation to be compatible with Cisco prestandard versions	GC
<code>spanning-tree forward-time</code>	Configures the spanning tree bridge forward time	GC
<code>spanning-tree hello-time</code>	Configures the spanning tree bridge hello time	GC
<code>spanning-tree max-age</code>	Configures the spanning tree bridge maximum age	GC
<code>spanning-tree mode</code>	Configures STP, RSTP or MSTP mode	GC
<code>spanning-tree mst configuration</code>	Changes to MSTP configuration mode	GC
<code>spanning-tree pathcost method</code>	Configures the path cost method for RSTP/MSTP	GC
<code>spanning-tree priority</code>	Configures the spanning tree bridge priority	GC
<code>spanning-tree system-bpdu-flooding</code>	Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled	GC
<code>spanning-tree transmission-limit</code>	Configures the transmission limit for RSTP/MSTP	GC
<code>max-hops</code>	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST
<code>mst priority</code>	Configures the priority of a spanning tree instance	MST
<code>mst vlan</code>	Adds VLANs to a spanning tree instance	MST
<code>name</code>	Configures the name for the multiple spanning tree	MST
<code>revision</code>	Configures the revision number for the multiple spanning tree	MST
<code>spanning-tree bpdu-filter</code>	Filters BPDUs for edge ports	IC
<code>spanning-tree bpdu-guard</code>	Shuts down an edge port if it receives a BPDU	IC
<code>spanning-tree cost</code>	Configures the spanning tree path cost of an interface	IC
<code>spanning-tree edge-port</code>	Enables fast forwarding for edge ports	IC
<code>spanning-tree link-type</code>	Configures the link type for RSTP/MSTP	IC
<code>spanning-tree loopback-detection</code>	Enables BPDU loopback detection for a port	IC

Table 90: Spanning Tree Commands (Continued)

Command	Function	Mode
<code>spanning-tree loopback-detection action</code>	Configures the response for loopback detection to block user traffic or shut down the interface	IC
<code>spanning-tree loopback-detection release-mode</code>	Configures loopback release mode for a port	IC
<code>spanning-tree loopback-detection trap</code>	Enables BPDU loopback SNMP trap notification for a port	IC
<code>spanning-tree mst cost</code>	Configures the path cost of an instance in the MST	IC
<code>spanning-tree mst port-priority</code>	Configures the priority of an instance in the MST	IC
<code>spanning-tree port-bpdu-flooding</code>	Floods BPDUs to other ports when global spanning tree is disabled	IC
<code>spanning-tree port-priority</code>	Configures the spanning tree priority of an interface	IC
<code>spanning-tree root-guard</code>	Prevents a designated port from passing superior BPDUs	IC
<code>spanning-tree spanning-disabled</code>	Disables spanning tree for an interface	IC
<code>spanning-tree tc-prop-stop</code>	Stops propagation of topology change information	IC
<code>spanning-tree loopback-detection release</code>	Manually releases a port placed in discarding state by loopback-detection	PE
<code>spanning-tree protocol-migration</code>	Re-checks the appropriate BPDU format	PE
<code>show spanning-tree</code>	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
<code>show spanning-tree mst configuration</code>	Shows the multiple spanning tree configuration	PE

spanning-tree This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[no] spanning-tree

Default Setting

Spanning tree is disabled.

Command Mode

Global Configuration

Command Usage

- ◆ The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one

route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

- ◆ When spanning tree is enabled globally by this command or enabled on an interface (`spanning-tree spanning-disabled` command), loopback detection is disabled.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree cisco-prestandard This command configures spanning tree operation to be compatible with Cisco prestandard versions. Use the **no** form to restore the default setting.

[no] spanning-tree cisco-prestandard

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Cisco prestandard versions prior to Cisco IOS Release 12.2(25)SEC do not fully follow the IEEE standard, causing some state machine procedures to function incorrectly. The command forces the spanning tree protocol to function in a manner compatible with Cisco prestandard versions.

Example

```
Console(config)#spanning-tree cisco-prestandard
Console(config)#
```

spanning-tree forward-time This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or $[(\text{max-age} / 2) + 1]$.

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a port will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax**spanning-tree hello-time** *time***no spanning-tree hello-time***time* - Time in seconds. (Range: 1-10 seconds).The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.**Default Setting**

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

Related Commands[spanning-tree forward-time \(433\)](#)[spanning-tree max-age \(435\)](#)

spanning-tree max-age This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or [2 x (hello-time + 1)].

The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

Related Commands

[spanning-tree forward-time \(433\)](#)

[spanning-tree hello-time \(434\)](#)

spanning-tree mode This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp** | **mstp**}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- ◆ **Spanning Tree Protocol**
This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.
- ◆ **Rapid Spanning Tree Protocol**
RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
 - **STP Mode** – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
 - **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
- ◆ **Multiple Spanning Tree Protocol**
 - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
 - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
 - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree mst configuration This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Setting

No VLANs are mapped to any MST instance.
The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

Related Commands

[mst vlan \(441\)](#)
[mst priority \(441\)](#)
[name \(442\)](#)
[revision \(443\)](#)
[max-hops \(440\)](#)

spanning-tree pathcost method This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

long - Specifies 32-bit based values that range from 1-200,000,000.
This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.

short - Specifies 16-bit based values that range from 1-65535.
This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

- ◆ The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost ([page 445](#)) takes precedence over port priority ([page 453](#)).

- ◆ The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

priority - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

spanning-tree system-bpdu-flooding This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the **no** form to restore the default.

Syntax

spanning-tree system-bpdu-flooding {to-all | to-vlan}

no spanning-tree system-bpdu-flooding

to-all - Floods BPDUs to all other ports on the switch.

to-vlan - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

Default Setting

Floods to all other ports in the same VLAN.

Command Mode

Global Configuration

Command Usage

The **spanning-tree system-bpdu-flooding** command has no effect if BPDU flooding is disabled on a port (see the [spanning-tree port-bpdu-flooding](#) command).

Example

```
Console(config)#spanning-tree system-bpdu-flooding to-all
Console(config)#
```

spanning-tree transmission-limit This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

max-hops This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops *hop-number*

no max-hops

hop-number - Maximum hop number for multiple spanning tree.
(Range: 1-40)

Default Setting

20

Command Mode

MST Configuration

Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```


mst priority This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance-id* **priority** *priority*

no mst *instance-id* **priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority of the a spanning tree instance.

(Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- ◆ MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- ◆ You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

mst vlan This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

[**no**] **mst** *instance-id* **vlan** *vlan-range*

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

vlan-range - Range of VLANs. (Range: 1-4094)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- ◆ Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- ◆ By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 64 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region ([page 442](#)) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

name This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

no name

name - Name of multiple spanning tree region. (Range: 1-32 alphanumeric characters)

Default Setting

Switch's MAC address

Command Mode

MST Configuration

Command Usage

The MST region name and revision number ([page 443](#)) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

Related Commands

[revision \(443\)](#)

revision This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

Syntax

revision *number*

no revision

number - Revision number of the spanning tree. (Range: 0-65535)

Default Setting

0

Command Mode

MST Configuration

Command Usage

The MST region name ([page 442](#)) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands

[name \(442\)](#)

spanning-tree bpd-filter This command allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree bpd-filter

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command stops all Bridge Protocol Data Units (BPDUs) from being transmitted on configured edge ports to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.
- ◆ BPDU filter can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto with the [spanning-tree edge-port](#) command).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

Related Commands[spanning-tree edge-port \(447\)](#)**spanning-tree
bpdu-guard**

This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form without any keywords to disable this feature, or with a keyword to restore the default settings.

Syntax**spanning-tree bpdu-guard** [**auto-recovery** [**interval** *interval*]]**no spanning-tree bpdu-guard** [**auto-recovery** [**interval**]]

auto-recovery - Automatically re-enables an interface after the specified interval.



Note: If the auto-recovery option is not set and bpdu guard detects a BPDU the edge port will be shutdown and must be manually recovered using the command, [no spanning-tree spanning-disabled](#) on the disabled interface.

interval - The time to wait before re-enabling an interface. (Range: 30-86400 seconds)

Default Setting

BPDU Guard: Disabled

Auto-Recovery: Disabled

Auto-Recovery Interval: 300 seconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker.
- ◆ If an interface is shut down by BPDU Guard, it must be manually re-enabled using the `no spanning-tree spanning-disabled` command if the auto-recovery interval is not specified.
- ◆ BPDU guard can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto with the `spanning-tree edge-port` command).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

Related Commands[spanning-tree edge-port \(447\)](#)[spanning-tree spanning-disabled \(455\)](#)

spanning-tree cost This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

Syntax**spanning-tree cost** *cost***no spanning-tree cost**

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method, 1-200,000,000 for long path cost method)¹⁰

Table 91: Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000

Table 91: Recommended STA Path Cost Range (Continued)

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 92: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- ◆ Path cost takes precedence over port priority.
- ◆ When the path cost method ([page 437](#)) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

10. Use the [spanning-tree pathcost method](#) command to set the path cost method. The range displayed in the CLI prompt message shows the maximum value for path cost. However, note that the switch still enforces the rules for path cost based on the specified path cost method (long or short).

spanning-tree edge-port This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port [auto]

no spanning-tree edge-port

auto - Automatically determines if an interface is an edge port.

Default Setting

Auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- ◆ When edge port is set as auto, the operational state is determined automatically by the Bridge Detection State Machine described in 802.1D-2004, where the edge port state may change dynamically based on environment changes (e.g., receiving a BPDU or not within the required interval).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

spanning-tree link-type This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {auto | point-to-point | shared}

no spanning-tree link-type

auto - Automatically derived from the duplex mode setting.

point-to-point - Point-to-point link.

shared - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- ◆ When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- ◆ RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree loopback-detection This command enables the detection and response to Spanning Tree loopback BPDU packets on the port. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree loopback-detection

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- ◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

**spanning-tree
loopback-detection
action**

This command configures the response for loopback detection to shut down the interface. Use the **no** form to restore the default.

Syntax

spanning-tree loopback-detection action {shutdown *duration*}

no spanning-tree loopback-detection action

shutdown - Shuts down the interface.

duration - The duration to shut down the interface.
(Range: 60-86400 seconds)

Default Setting

shutdown, 60 seconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If an interface is shut down by this command, and the release mode is set to "auto" with the [spanning-tree loopback-detection release-mode](#) command, the selected interface will be automatically enabled when the shutdown interval has expired.
- ◆ If an interface is shut down by this command, and the release mode is set to "manual," the interface can be re-enabled using the [spanning-tree loopback-detection release](#) command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
Console(config-if)#
```

spanning-tree loopback-detection release-mode This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the **no** form to restore the default.

Syntax

spanning-tree loopback-detection release-mode {auto | manual}

no spanning-tree loopback-detection release-mode

auto - Allows a port to automatically be released from the discarding state when the loopback state ends.

manual - The port can only be released from the discarding state manually.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If the port is configured for automatic loopback release, the port will be returned to the forwarding state when the interval for the parameter "spanning-tree loopback-detection action shutdown *duration*" has expired.
- ◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- ◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.
- ◆ When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the **spanning-tree loopback-detection release** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```

spanning-tree loopback-detection trap This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the **no** form to restore the default.

Syntax

[no] spanning-tree loopback-detection trap

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method¹¹, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in [Table 91 on page 445](#).

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in [Table 92 on page 446](#).

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Each spanning-tree instance is associated with a unique set of VLAN IDs.
- ◆ This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to

¹¹. Use the [spanning-tree pathcost method](#) command to set the path cost method.

interfaces attached to faster media, and higher values assigned to interfaces with slower media.

- ◆ Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- ◆ Path cost takes precedence over interface priority.

Example

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

[spanning-tree mst port-priority \(452\)](#)

spanning-tree mst port-priority This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority for an interface. (Range: 0-240 in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- ◆ Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands[spanning-tree mst cost \(451\)](#)

spanning-tree port-bpdu-flooding This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the **no** form to restore the default setting.

Syntax**[no] spanning-tree port-bpdu-flooding****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the [spanning-tree system-bpdu-flooding](#) command.
- ◆ The [spanning-tree system-bpdu-flooding](#) command has no effect if BPDU flooding is disabled on a port by the **spanning-tree port-bpdu-flooding** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

spanning-tree port-priority This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax**spanning-tree port-priority *priority*****no spanning-tree port-priority***priority* - The priority for a port. (Range: 0-240, in steps of 16)**Default Setting**

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- ◆ Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
- ◆ The criteria used for determining the port role is based on root bridge ID, root path cost, designated bridge, designated port, port priority, and port number, in that order and as applicable to the role under question.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

[spanning-tree cost \(445\)](#)

spanning-tree root-guard This command prevents a designated port from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree root-guard

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- ◆ When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- ◆ Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It

could also be used to form a border around part of the network where the root bridge is allowed.

- ◆ When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

spanning-tree spanning-disabled This command disables the spanning tree algorithm for the specified interface. Use the **no** form to re-enable the spanning tree algorithm for the specified interface.

Syntax

[no] spanning-tree spanning-disabled

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When spanning tree is enabled globally (**spanning-tree** command) or enabled on an interface by this command, loopback detection is disabled.

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree tc-prop-stop This command stops the propagation of topology change notifications (TCN). Use the **no** form to allow propagation of TCN messages.

Syntax

[no] spanning-tree tc-prop-stop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When this command is enabled on an interface, topology change information originating from the interface will still be propagated.

This command should not be used on an interface which is purposely configured in a ring topology.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#spanning-tree tc-prop-stop
Console(config-if)#
```

**spanning-tree
loopback-detection
release**

This command manually releases a port placed in discarding state by loopback-detection.

Syntax

spanning-tree loopback-detection release *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

Use this command to release an interface from discarding state if loopback detection release mode is set to “manual” by the [spanning-tree loopback-detection release-mode](#) command and BPDU loopback occurs.

Example

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```


spanning-tree protocol-migration This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

show spanning-tree This command shows the configuration for the common spanning tree (CST), for all instances within the multiple spanning tree (MST), or for a specific instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance-id* | **brief** | **stp-enabled-only**]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

instance-id - Instance identifier of the multiple spanning tree.
(Range: 0-4094)

brief - Shows a summary of global and interface settings.

stp-enabled-only - Displays global settings, and settings for interfaces for which STP is enabled.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- ◆ Use the **show spanning-tree interface** command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- ◆ Use the **show spanning-tree mst** command to display the spanning tree configuration for all instances within the Multiple Spanning Tree (MST), including global settings and settings for active interfaces.
- ◆ Use the **show spanning-tree mst instance-id** command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST), including global settings and settings for all interfaces.

Example

```

Console#show spanning-tree
Spanning Tree Information
-----
Spanning Tree Mode           : MSTP
Spanning Tree Enabled/Disabled : Enabled
Instance                     : 0
VLANs Configured             : 1-4094
Priority                      : 32768
Bridge Hello Time (sec.)      : 2
Bridge Max. Age (sec.)        : 20
Bridge Forward Delay (sec.)    : 15
Root Hello Time (sec.)        : 2
Root Max. Age (sec.)          : 20
Root Forward Delay (sec.)      : 15
Max. Hops                     : 20
Remaining Hops                : 20
Designated Root               : 32768.0.0001ECF8D8C6
Current Root Port              : 21
Current Root Cost              : 100000
Number of Topology Changes     : 5
Last Topology Change Time (sec.): 11409
Transmission Limit             : 3
Path Cost Method               : Long
Flooding Behavior              : To VLAN
Cisco Prestandard              : Disabled
-----
Eth 1/ 1 Information
-----
Admin Status                  : Enabled
Role                          : Disabled

```

```

State : Discarding
External Admin Path Cost : 0
Internal Admin Path Cost : 0
External Oper Path Cost : 100000
Internal Oper Path Cost : 100000
Priority : 128
Designated Cost : 100000
Designated Port : 128.1
Designated Root : 32768.0.0001ECF8D8C6
Designated Bridge : 32768.0.123412341234
Forward Transitions : 4
Admin Edge Port : Disabled
Oper Edge Port : Disabled
Admin Link Type : Auto
Oper Link Type : Point-to-point
Flooding Behavior : Enabled
Spanning-Tree Status : Enabled
Loopback Detection Status : Enabled
Loopback Detection Release Mode : Auto
Loopback Detection Trap : Disabled
Loopback Detection Action : Block
Root Guard Status : Disabled
BPDU Guard Status : Disabled
BPDU Guard Auto Recovery : Disabled
BPDU Guard Auto Recovery Interval : 300
BPDU Filter Status : Disabled
TC Propagate Stop : Disabled
.
.
.

```

This example shows a brief summary of global and interface setting for the spanning tree.

```

Console#show spanning-tree brief
Spanning Tree Mode : RSTP
Spanning Tree Enabled/Disabled : Enabled
Designated Root : 32768.0000E8944000
Current Root Port (Eth) : 1/24
Current Root Cost : 10000

Interface Pri Designated      Designated Oper   STP   Role State Oper
              Bridge ID      Port ID   Cost   Status      Role State Oper
-----
Eth 1/ 1  128 32768.0000E89382A0  128.1      100000  EN     DESG FWD  No
Eth 1/ 2  128 32768.0000E89382A0  128.2      10000   EN     DISB BLK  No
Eth 1/ 3  128 32768.0000E89382A0  128.3      10000   EN     DISB BLK  No
Eth 1/ 4  128 32768.0000E89382A0  128.4      10000   EN     DISB BLK  No
Eth 1/ 5  128 32768.0000E89382A0  128.5      10000   EN     DISB BLK  No
.
.
.

```

show spanning-tree mst configuration This command shows the configuration of the multiple spanning tree.

Command Mode
Privileged Exec

Example

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-----
Configuration Name : R&D
Revision Level      :0

Instance VLANs
-----
      0      1-4094
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 93: VLAN Commands

Command Group	Function
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, and PVID
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring IEEE 802.1Q Tunneling	Configures 802.1Q Tunneling (QinQ Tunneling)
Configuring Protocol-based VLANs*	Configures protocol-based VLANs based on frame type and protocol
Configuring MAC Based VLANs*	Configures MAC-based VLANs
Configuring Voice VLANs	Configures VoIP traffic detection and enables a Voice VLAN

* If a packet matches the rules defined by more than one of these functions, only one of them is applied, with the precedence being MAC-based, protocol-based, and then native port-based (see the [switchport priority default](#) command).

Editing VLAN Groups

Table 94: Commands for Editing VLAN Groups

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC

vlan database This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the `show vlan` command.
- ◆ Use the `interface vlan` command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the `show running-config` command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

`show vlan (470)`

vlan This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}] [**rspan**]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

media ethernet - Ethernet media type.

state - Keyword to be followed by the VLAN state.

active - VLAN is operational.

suspend - VLAN is suspended. Suspended VLANs do not pass packets.

rspan - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPAN cannot include VLAN 1 (the switch's default VLAN). Nor should it include VLAN 4093 (which is used for switch clustering). Configuring VLAN 4093 for other purposes may cause problems in the Clustering operation. For more information on configuring RSPAN through the CLI, see ["RSPAN Mirroring Commands" on page 405](#).

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- ◆ **no vlan** *vlan-id* deletes the VLAN.
- ◆ **no vlan** *vlan-id* **name** removes the VLAN name.
- ◆ **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- ◆ You can configure up to 4094 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

[show vlan \(470\)](#)

Configuring VLAN Interfaces

Table 95: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport forbidden vlan	Adds VLANs to a forbidden list for an interface	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport mode	Configures VLAN membership mode for an interface	IC

Table 95: Commands for Configuring VLAN Interfaces (Continued)

Command	Function	Mode
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC
switchport priority default	Sets a port priority for incoming untagged frames	IC

interface vlan This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface. Use the **no** form to change a Layer 3 normal VLAN back to a Layer 2 interface.

Syntax

[no] interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Creating a “normal” VLAN with the [vlan](#) command initializes it as a Layer 2 interface. To change it to a Layer 3 interface, use the [interface](#) command to enter interface configuration for the desired VLAN, enter any Layer 3 configuration commands, and save the configuration settings.
- ◆ To change a Layer 3 normal VLAN back to a Layer 2 VLAN, use the [no interface](#) command.

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

[shutdown \(356\)](#)

[interface \(350\)](#)

[vlan \(462\)](#)

switchport acceptable-frame-types This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

all - The port accepts all frames, tagged or untagged.

tagged - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

[switchport mode \(468\)](#)

switchport allowed vlan This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {vlan-list | add vlan-list [tagged | untagged] | remove vlan-list}

no switchport allowed vlan

vlan-list - If a VLAN list is entered without using the **add** option, the interface is assigned to the specified VLANs, and membership in all previous VLANs is removed. The interface is added as a tagged member if [switchport mode](#) is set to hybrid or access, or as an untagged member if switchport mode is set to trunk.

Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

add *vlan-list* - List of VLAN identifiers to add. When the **add** option is used, the interface is assigned to the specified VLANs, and membership in all previous VLANs is retained.

remove *vlan-list* - List of VLAN identifiers to remove.

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If a port or trunk has switchport mode set to **access**, then only one VLAN can be added with this command. If a VLAN list is specified, only the last VLAN in the list will be added to the interface.
- ◆ A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- ◆ If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- ◆ Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- ◆ If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- ◆ If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan Use this command to prevent a port from dynamically joining a VLAN. Use the **no** form of the command to disable all restrictions.

Syntax

switchport forbidden vlan {add *vlan-list* | remove *vlan-list*}

no switchport forbidden vlan

add *vlan-list* - List of VLAN identifiers to add to the forbidden list.
When the **add** option is used, the interface is prevented from being dynamically added to the specified VLANs.

remove *vlan-list* - List of VLAN identifiers to remove from the forbidden list.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

If a VLAN on the allowed list for an interface is manually added to the forbidden list for the interface, the VLAN is automatically removed from the allowed list for that interface.

Example

The following example shows how to add VLANs 300 and 600 to the forbidden list for port 2:

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport forbidden vlan add 300,600
Console(config-if)#
```

switchport ingress-filtering This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[no] switchport ingress-filtering

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Ingress filtering only affects tagged frames.
- ◆ If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- ◆ If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- ◆ Ingress filtering does not affect VLAN independent BPDU frames, such as STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport mode This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {access | hybrid | trunk}

no switchport mode

access - Specifies an access VLAN interface. The port transmits and receives untagged frames on a single VLAN only.

hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

trunk - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

Default Setting

Hybrid mode, with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

[switchport acceptable-frame-types \(465\)](#)

switchport native vlan This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.
- ◆ If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

Displaying VLAN Information

This section describes commands used to display VLAN information.

Table 96: Commands for Displaying VLAN Information

Command	Function	Mode
<code>show interfaces status vlan</code>	Displays status for the specified VLAN interface	NE, PE
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE
<code>show vlan</code>	Shows VLAN information	NE, PE

show vlan This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID:          1
Type:              Static
Name:              DefaultVlan
Status:            Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                      Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                      Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                      Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                      Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                      Eth1/26(S)

Console#
```

Configuring IEEE 802.1Q Tunneling

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 97: 802.1Q Tunneling Commands

Command	Function	Mode
<code>dot1q-tunnel system-tunnel-control</code>	Configures the switch to operate in normal mode or QinQ mode	GC
<code>dot1q-tunnel tpid</code>	Configures the other tag ethertype for QinQ tunneling.	GC
<code>switchport dot1q-tunnel mode</code>	Configures an interface as a QinQ tunnel port	IC
<code>switchport dot1q-tunnel priority map</code>	Copies inner tag priority to outer tag priority	IC
<code>show dot1q-tunnel</code>	Displays the 802.1Q settings	PE
<code>show interfaces switchport</code>	Displays port QinQ operational status	PE

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (`dot1q-tunnel system-tunnel-control`).
2. Create a SPVLAN (`vlan`).
3. To configure QinQ tunnel access ports use the interface configuration command `switchport dot1q-tunnel mode access` (See `switchport dot1q-tunnel mode`).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See `dot1q-tunnel tpid`.)
5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (`switchport allowed vlan`).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (`switchport native vlan`).

7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode ([switchport dot1q-tunnel mode](#)).
8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member ([switchport allowed vlan](#)).

Limitations for QinQ

- ◆ The native VLAN for the tunnel uplink ports and tunnel access ports cannot be the same. However, the same service VLANs can be set on both tunnel port types.
- ◆ IGMP Snooping should not be enabled on a tunnel access port.
- ◆ If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel uplink port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

dot1q-tunnel system-tunnel-control This command sets the switch to operate in QinQ mode. Use the **no** form to disable QinQ operating mode.

Syntax

[no] dot1q-tunnel system-tunnel-control

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

Related Commands

[show dot1q-tunnel \(475\)](#)

[show interfaces switchport \(365\)](#)

dot1q-tunnel tpid Use this command to set the global setting for the QinQ outer tag ethertype field. Use the no form of the command to set the ethertype field to the default value.

Syntax

[no] dot1q-tunnel tpid *ethertype*

ethertype – A specific Ethernet protocol number. (Range: 800-ffff hex)

Default Setting

The ethertype is set to 0x8100

Command Mode

Global Configuration

Command Usage

Use the dot1q-tunnel tpid command to set the global custom 802.1Q ethertype. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the global 802.1Q ethertype, incoming frames on trunk ports containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field. Frames arriving on trunk ports containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of the port.

The specified ethertype only applies to ports configured in Uplink mode using the switchport dot1q-tunnel mode command. If the port is in normal mode (i.e., unspecified), the TPID is always 0x8100. If the port is in Access mode, received packets are processed as untagged packets.

Example

```
Console(config)#dot1q-tunnel tpid 0x88A8
Console(config)#
```

Related Commands

[show dot1q-tunnel \(475\)](#)

[switchport dot1q-tunnel mode \(474\)](#)

switchport dot1q-tunnel mode This command configures an interface as a QinQ tunnel port. Use the **no** form to disable QinQ on the interface.

Syntax

switchport dot1q-tunnel mode {access | uplink}

no switchport dot1q-tunnel mode

access – Sets the port as an 802.1Q tunnel access port.

uplink – Sets the port as an 802.1Q tunnel uplink port.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ QinQ tunneling must be enabled on the switch using the [dot1q-tunnel system-tunnel-control](#) command before the **switchport dot1q-tunnel mode** interface command can take effect.
- ◆ When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider's tag added to the outer tag.
- ◆ When a tunnel uplink port receives a packet from the service provider, the outer service provider's tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

Related Commands

[show dot1q-tunnel \(475\)](#)

[show interfaces switchport \(365\)](#)

switchport dot1q-tunnel priority map This command copies the inner tag priority to the outer tag priority. Use the **no** form to disable this feature.

Syntax

[no] switchport dot1q-tunnel priority map

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel priority map
Console(config-if)#
```

show dot1q-tunnel This command displays information about 802.1Q settings.

Syntax

show dot1q-tunnel

Default Setting

None

Command Mode

Privileged Exec.

Example

```
Console#show dot1q-tunnel
802.1Q Tunnel Status : Enabled
802.1Q Tunnel TPID   : FFFF (Hex)
```

Port	Mode	Priority Mapping
Eth 1/ 1	Normal	Disabled
Eth 1/ 2	Uplink	Enabled
Eth 1/ 3	Normal	Disabled
Eth 1/ 4	Normal	Disabled
Eth 1/ 5	Normal	Disabled
Eth 1/ 6	Normal	Disabled
Eth 1/ 7	Normal	Disabled
Eth 1/ 8	Normal	Disabled
Eth 1/ 9	Normal	Disabled
Eth 1/10	Normal	Disabled
Eth 1/11	Normal	Disabled
Eth 1/12	Normal	Disabled
Eth 1/13	Normal	Disabled
Eth 1/14	Normal	Disabled
Eth 1/15	Normal	Disabled
Eth 1/16	Normal	Disabled

```
Eth 1/17 Normal Disabled
Eth 1/18 Normal Disabled
Eth 1/19 Normal Disabled
Eth 1/20 Normal Disabled
Eth 1/21 Normal Disabled
Eth 1/22 Normal Disabled
Eth 1/23 Normal Disabled
Eth 1/24 Normal Disabled
Eth 1/25 Normal Disabled
Eth 1/26 Normal Disabled
Eth 1/27 Normal Disabled
Eth 1/28 Normal Disabled
Console#
```

Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 98: Protocol-based VLAN Commands

Command	Function	Mode
<code>protocol-vlan protocol-group</code>	Create a protocol group, specifying the supported protocols	GC
<code>protocol-vlan protocol-group</code>	Maps a protocol group to a VLAN	IC
<code>show protocol-vlan protocol-group</code>	Shows the configuration of protocol groups	PE
<code>show interfaces protocol-vlan protocol-group</code>	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use ([page 462](#)). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the `protocol-vlan protocol-group` command (Global Configuration mode).

3. Then map the protocol for each interface to the appropriate VLAN using the `protocol-vlan protocol-group` command (Interface Configuration mode).

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{**add** | **remove**}
frame-type *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

*frame*¹² - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

protocol - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: arp, ip, ipv6, rarp.

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet  
protocol-type ip  
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet  
protocol-type arp  
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id* **priority** *priority*

no protocol-vlan protocol-group *group-id* **vlan**

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

vlan-id - VLAN to which matching protocol traffic is forwarded.
(Range: 1-4094)

12. SNAP frame types are not supported by this switch due to hardware limitations.

priority - The priority assigned to untagged ingress traffic.
(Range: 0-7, where 7 is the highest priority)

Default Setting

No protocol groups are mapped for any interface.

Priority: 0

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the `vlan` command), these interfaces will admit traffic of any protocol type into the associated VLAN.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- ◆ When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
 - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
 - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
 - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2 priority 0
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Setting

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

Protocol Group ID   Frame Type   Protocol Type
-----
                  1       ethernet    08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group
Port      Protocol Group ID VLAN ID Priority
-----
Eth 1/1           1   vlan2         0
Console#
```

Configuring MAC Based VLANs

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 99: MAC Based VLAN Commands

Command	Function	Mode
<code>mac-vlan</code>	Defines the IP Subnet VLANs	GC
<code>show mac-vlan</code>	Displays IP Subnet VLAN settings	PE

mac-vlan This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

Syntax

mac-vlan mac-address mac-address [mask mask-address] vlan vlan-id
[priority priority]

no mac-vlan mac-address {mac-address [mask mask-address] | all}

mac-address – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

mask-address - Identifies a range of MAC addresses. The mask can be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx, where an equivalent binary value "1" means relevant and "0" means ignore.

vlan-id – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The MAC-to-VLAN mapping applies to all ports on the switch.

- ◆ Source MAC addresses can be mapped to only one VLAN ID.
- ◆ Configured MAC addresses cannot be broadcast or multicast addresses.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- ◆ The binary equivalent mask matching the characters in the front of the first non-zero character must all be 1s (e.g., 111, i.e., it cannot be 101 or 001...). A mask for the MAC address: 00-50-6e-00-5f-b1 translated into binary:
MAC: 00000000-01010000-01101110-00000000-01011111-10110001
could be: 11111111-11xxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
So the mask in hexadecimal for this example could be:
ff-fx-xx-xx-xx-xx/ff-c0-00-00-00-00/ff-e0-00-00-00-00

Example

The following example assigns traffic from source MAC address 00-00-00-11-22-33 to VLAN 10.

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 mask FF-FF-FF-FF-00-00
vlan 10
Console(config)#
```

show mac-vlan This command displays MAC address-to-VLAN assignments.

Command Mode

Privileged Exec

Command Usage

Use this command to display MAC address-to-VLAN mappings.

Example

The following example displays all configured MAC address-based VLANs.

```
Console#show mac-vlan
MAC Address      VLAN ID  Priority
-----
00-00-00-11-22-33    10      0
Console#
```

Configuring Voice VLANs

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port to the Voice VLAN. Alternatively, switch ports can be manually configured.

Table 100: Voice VLAN Commands

Command	Function	Mode
<code>voice vlan</code>	Defines the Voice VLAN ID	GC
<code>voice vlan aging</code>	Configures the aging time for Voice VLAN ports	GC
<code>voice vlan mac-address</code>	Configures VoIP device MAC addresses	GC
<code>switchport voice vlan</code>	Sets the Voice VLAN port mode	IC
<code>switchport voice vlan priority</code>	Sets the VoIP traffic priority for ports	IC
<code>switchport voice vlan rule</code>	Sets the automatic VoIP traffic detection method for ports	IC
<code>switchport voice vlan security</code>	Enables Voice VLAN security on ports	IC
<code>show voice vlan</code>	Displays Voice VLAN settings	PE

voice vlan This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

Syntax

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.

- ◆ VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.
- ◆ Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.
- ◆ The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the [switchport voice vlan](#) command).

Example

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

Syntax

voice vlan aging *minutes*

no voice vlan

minutes - Specifies the port Voice VLAN membership time out.
(Range: 5-43200 minutes)

Default Setting

1440 minutes

Command Mode

Global Configuration

Command Usage

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

The VoIP aging time starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from the voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the voice VLAN aging time.

Note that when the `switchport voice vlan` command is set to auto mode, the remaining aging time displayed by the `show voice vlan` command will be displayed. Otherwise, if the `switchport voice vlan` command is disabled or set to manual mode, the remaining aging time will display "NA."

Example

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan mac-address This command specifies MAC address ranges to add to the OUI Telephony list. Use the **no** form to remove an entry from the list.

Syntax

voice vlan mac-address *mac-address* **mask** *mask-address*
[**description** *description*]

no voice vlan mac-address *mac-address* **mask** *mask-address*

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (Format: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx; for example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-30 characters, use double quotation marks if a space character is included.)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.
- ◆ Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting a mask of FF-FF-FF-FF-FF-FF specifies a single MAC address.

Example

The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-00 description "A new phone"
Console(config)#
```

switchport voice vlan This command specifies the Voice VLAN mode for ports. Use the **no** form to disable the Voice VLAN feature on the port.

Syntax

switchport voice vlan {manual | auto}

no switchport voice vlan

manual - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

auto - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1AB (LLDP) using the [switchport voice vlan rule](#) command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the [voice vlan mac-address](#) command.
- ◆ All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), ensure that VLAN membership is not set to access mode using the [switchport mode](#) command.

Example

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority This command specifies a CoS priority for VoIP traffic on a port. Use the **no** form to restore the default priority on a port.

Syntax

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (Range: 0-6)

Default Setting

6

Command Mode

Interface Configuration

Command Usage

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

Example

The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

Syntax

[no] switchport voice vlan rule {oui | lldp}

oui - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

lldp - Uses LLDP to discover VoIP devices attached to the port.

Default Setting

OUI: Enabled

LLDP: Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the [voice vlan mac-address](#) command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
- ◆ LLDP checks that the “telephone bit” in the system capability TLV is turned on. See [“LLDP Commands” on page 573](#) for more information on LLDP.

Example

The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security This command enables security filtering for VoIP traffic on a port. Use the **no** form to disable filtering on a port.

Syntax

[no] switchport voice vlan security

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- ◆ When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list ([voice vlan mac-address](#)).

Example

The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

Syntax

show voice vlan {oui | status}

oui - Displays the OUI Telephony list.

status - Displays the global and port Voice VLAN settings.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

When the **switchport voice vlan** command is set to auto mode, the remaining aging time displayed by the **show voice vlan** command will be displayed (or "Not Start" will be displayed). Otherwise, if the switchport voice vlan command is disabled or set to manual mode, the remaining aging time will display "NA."



Note: When the aging time shows <1, the remaining time is less than 1 minute.

Example

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status      : Enabled
Voice VLAN ID          : 1234
Voice VLAN aging time  : 1440 minutes
```

```
Voice VLAN Port Summary
Port      Mode      Security Rule      Priority Remaining Age
                                   (minutes)
-----
Eth 1/ 1 Auto      Enabled OUI                6 100
Eth 1/ 2 None      Disabled OUI         6 NA
Eth 1/ 3 Manual    Enabled OUI         5 NA
Eth 1/ 4 Auto      Disabled OUI         6 Not Start
Eth 1/ 5 None      Disabled OUI         6 NA
Eth 1/ 6 None      Disabled OUI         6 NA
Eth 1/ 7 None      Disabled OUI         6 NA
Eth 1/ 8 None      Disabled OUI         6 NA
Eth 1/ 9 None      Disabled OUI         6 NA
Eth 1/10 None      Disabled OUI         6 NA
```

```
Console#show voice vlan oui
OUI Address      Mask      Description
-----
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone
```

```
Console#
```


Class of Service Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the switch's priority queues can be configured.

Table 101: Priority Commands

Command Group	Function
Priority Commands (Layer 2)	Configures the queue mode, queue weights, and default priority for untagged frames
Priority Commands (Layer 3 and 4)	Sets the default priority processing method (CoS or DSCP), maps priority tags for internal processing, maps values from internal priority table to CoS values used in tagged egress packets for Layer 2 interfaces, maps internal per hop behavior to hardware queues

Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 102: Priority Commands (Layer 2)

Command	Function	Mode
<code>queue mode</code>	Sets the queue mode to Weighted Round-Robin (WRR), strict priority, or a combination of strict and weighted queuing	IC
<code>queue weight</code>	Assigns round-robin weights to the priority queues	IC
<code>switchport priority default</code>	Sets a port priority for incoming untagged frames	IC
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	PE
<code>show queue mode</code>	Shows the current queue mode	PE
<code>show queue weight</code>	Shows weights assigned to the weighted queues	PE

queue mode This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr** | **strict-wrr** [*queue-type-list*]}

no queue mode

strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the [queue weight](#) command), and servicing each queue in a round-robin fashion.

strict-wrr - Uses strict or weighted service as specified for each queue.

queue-type-list - Indicates if the queue is a normal or strict type.
(Options: 0 indicates a normal queue, 1 indicates a strict queue)

Default Setting

WRR

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queuing.
- ◆ Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- ◆ Weighted Round Robin (WRR) uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the [queue weight](#) command to assign weights for WRR queuing to the eight priority queues.
- ◆ If Strict and WRR mode is selected, a combination of strict and weighted service is used as specified for each queue. The queues assigned to use strict or WRR priority should be specified using the *queue-type-list* parameter.
- ◆ A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

- ◆ Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.
- ◆ The specified queue mode applies to all interfaces.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue mode strict
Console(config-if)#
```

Related Commands

[queue weight \(491\)](#)

[show queue mode \(493\)](#)

queue weight This command assigns weights to the eight class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the **no** form to restore the default weights.

Syntax

queue weight *weight0...weight7*

no queue weight

weight0...weight7 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1-255)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command shares bandwidth at the egress port by defining scheduling weights for Weighted Round-Robin, or for the queuing mode that uses a combination of strict and weighted queuing ([page 490](#)).
- ◆ Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

Example

The following example shows how to assign round-robin weights of 1 - 8 to the CoS priority queues 0 - 7.

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue weight 1 2 3 4 5 6 7 8
Console(config-if)#
```

Related Commands

[queue mode \(490\)](#)

[show queue weight \(493\)](#)

switchport priority default This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The precedence for priority mapping is IP DSCP, and then default switchport priority.
- ◆ The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- ◆ The switch provides eight priority queues for each port. It can be configured to use strict priority queuing, Weighted Round Robin (WRR), or a combination of strict and weighted queuing using the [queue mode](#) command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 2 of the output

port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

Related Commands

[show interfaces switchport \(365\)](#)

show queue mode This command shows the current queue mode.

Syntax

show queue mode [*interface*]

interface

ethernet *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

```
Console#show queue mode
Unit  Port  queue mode
----  -
    1      1  Weighted Round Robin
...
```

show queue weight This command displays the weights used for the weighted queues.

Syntax

show queue weight [*interface*]

interface

ethernet *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode
Privileged Exec

Example

```
Console#show queue weight
Information of Eth 1/1
Queue ID  Weight
-----  -
          0      1
          1      2
          2      4
          3      6
          4      8
          5     10
          6     12
          7     14
...

```

Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 103: Priority Commands (Layer 3 and 4)

Command	Function	Mode
<code>qos map cos-queue</code>	Maps CoS/CFI values in incoming packets to per-hop behavior, or the queue used for this router hop	IC
<code>qos map dscp-queue</code>	Maps DSCP values in incoming packets to per-hop behavior, or the queue used for this router hop	IC
<code>qos map trust-mode</code>	Sets QoS mapping to DSCP or CoS	IC
<code>show qos map cos-queue</code>	Shows ingress CoS to egress queue map	PE
<code>show qos map dscp-queue</code>	Shows ingress DSCP to egress queue map	PE
<code>show qos map trust-mode</code>	Shows the QoS mapping mode	PE

* The default settings used for mapping priority values to internal DSCP values and back to the hardware queues are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings unless a queuing problem occurs with a particular application.

qos map cos-queue This command maps CoS/CFI values in incoming packets to per-hop behavior for priority processing. Use the **no** form to restore the default settings.

Syntax

qos map cos-queue *queue* **from** *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

queue - Per-hop behavior, or the priority used for this router hop.
(Range: 0-7)

cos - CoS value in ingress packets. (Range: 0-7)

cfi - Canonical Format Indicator. Set this parameter to "0" to indicate that the MAC address information carried in the frame is in canonical format.
(Range: 0-1)

Default Setting

Table 104: Default Mapping of CoS/CFI Values to Queue/CFI

CoS	CFI	0	1
0		2	2
1		0	0
2		1	1
3		3	3
4		4	4
5		5	5
6		6	6
7		7	7

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The default mapping of CoS/CFI to Queue/CFI values shown in [Table 104](#) is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.
- ◆ Enter a value for the per-hop behavior, followed by the keyword "from" and then up to eight CoS/CFI paired values separated by spaces.
- ◆ If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-Queue mapping table is used to generate priority for processing. Note that priority tags in the original packet are not modified by this command.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#qos map cos-dscp 0 0 from 0 1
Console(config-if)#
```

qos map dscp-queue This command maps DSCP values in incoming packets to per-hop behavior for priority processing. Use the **no** form to restore the default settings.

Syntax

qos map dscp-queue *dscp-queue* **from** *dscp0 ... dscp7*

no qos map dscp-queue *dscp0 ... dscp7*

dscp-queue - Per-hop behavior, or the priority used for this router hop.
(Range: 0-7)

dscp - DSCP value in ingress packets. (Range: 0-63)

DEFAULT SETTING

Table 105: Default Mapping of DSCP Values to Queue

	d2	0	1	2	3	4	5	6	7	8	9
d1											
0		2	2	2	2	2	2	2	2	0	0
1		0	0	0	0	0	0	1	1	1	1
2		1	1	1	1	3	3	3	3	3	3
3		3	3	4	4	4	4	4	4	4	4
4		5	5	5	5	5	5	5	5	6	6
5		6	6	6	6	6	6	7	7	7	7
6		7	7	7	7						

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Enter a value for the per-hop behavior, followed by the keyword “from” and then up to eight DSCP values separated by spaces.
- ◆ This map is only used when the QoS mapping mode is set to “DSCP” by the **qos map trust-mode** command, and the ingress packet type is IPv4.
- ◆ Two QoS domains can have different DSCP definitions, so the DSCP-to-Queue/ map can be used to modify one set of DSCP values to match the definition of another domain. This map should be applied at the receiving port at the boundary of a QoS administrative domain.

Example

This example changes the priority for all packets entering port 1 which contain a DSCP value of 1 to a per-hop behavior of 3.

```
Console(config)#interface ethernet 1/2
Console(config-if)#qos map dscp-queue 3 from 1
Console(config-if)#
```

qos map trust-mode This command sets QoS mapping to DSCP or CoS. Use the **no** form to restore the default setting.

Syntax

qos map trust-mode {dscp | cos}

no qos map trust-mode

dscp - Sets the QoS mapping mode to DSCP.

cos - Sets the QoS mapping mode to CoS.

Default Setting

CoS

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- ◆ If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see [page 492](#)) is used for priority processing.
- ◆ If the QoS mapping mode is set to CoS with this command, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

For an untagged packet, the default port priority (see [page 492](#)) is used for priority processing.

Example

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

```
Console(config)#interface 1/1
Console(config-if)#qos map trust-mode cos
Console(config-if)#
```

show qos map cos-queue This command shows the ingress CoS to egress queue map.

Syntax

show qos map cos-queue interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

```
Console#show qos map cos-queue interface ethernet 1/1
CoS Information of Eth 1/1
CoS-Queue map.
CoS   : CFI   0           1
-----
0           2           2
1           0           0
2           1           1
3           3           3
4           4           4
5           5           5
6           6           6
7           7           7

Console#
```

show qos map dscp-queue This command shows the ingress DSCP to egress queue map.

Syntax

show qos map dscp-queue interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Command Usage

This map is only used when the QoS mapping mode is set to "DSCP" by the **qos map trust-mode** command, and the ingress packet type is IPv4.

Example

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, $\text{ingress-dscp} = \text{ingress-dscp10} * 10 + \text{ingress-dscp1}$); and the corresponding dscp is shown at the intersecting cell in the table.

```
Console#show qos map dscp-queue interface ethernet 1/1
Information of Eth 1/1
DSCP to queue map.
d1:d2  0  1  2  3  4  5  6  7  8  9
-----
0  :  2  2  2  2  2  2  2  2  0  0
1  :  0  0  0  0  0  0  1  1  1  1
2  :  1  1  1  1  3  3  3  3  3  3
3  :  3  3  4  4  4  4  4  4  4  4
4  :  5  5  5  5  5  5  5  5  6  6
5  :  6  6  6  6  6  6  7  7  7  7
6  :  7  7  7  7  7  7  7  7  7  7

Console#
```

show qos map trust-mode This command shows the QoS mapping mode.

Syntax

show qos map trust-mode interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

Command Mode

Privileged Exec

Example

The following shows that the trust mode is set to CoS:

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
  CoS Map Mode:          CoS mode
Console#
```

Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 106: Quality of Service Commands

Command	Function	Mode
class-map	Creates a class map for a type of traffic	GC
description	Specifies the description of a class map	CM
match	Defines the criteria used to classify traffic	CM
rename	Redefines the name of a class map	CM
policy-map	Creates a policy map for multiple interfaces	GC
description	Specifies the description of a policy map	PM
class	Defines a traffic classification for the policy to act on	PM
rename	Redefines the name of a policy map	PM
police rate	Defines an enforcer for classified traffic based on the metered flow rate	PM-C
set cos	Serves IP traffic by setting a class of service value for matching packets for internal processing	PM-C
set ip dscp	Modifies the DSCP value in matching packets.	PM-C
service-policy	Applies a policy map defined by the policy-map command to a particular interface	IC
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE
show policy-map	Displays the QoS policy maps which define classification criteria for ingress or egress traffic, and may include policers for bandwidth limitations	PE
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the [class-map](#) command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the [match](#) command to select a specific type of traffic based on an access list, an IPv4 DSCP value, IPv4 Precedence value, IPv6 DSCP value, a VLAN, or a

CoS value. Note that a class map can include match settings for both IP values and a VLAN.

3. Use the **policy-map** command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
4. Use the **class** command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain up to 16 class maps.
5. Use the **set cos** command to modify the per-hop behavior, the class of service value in the VLAN tag for the matching traffic class, and use one of the **police** commands to monitor parameters such as the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
6. Use the **service-policy** command to assign a policy map to a specific interface.



Note: Create a Class Map before creating a Policy Map.

class-map This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map.

Syntax

[no] class-map *class-map-name* [**match-any**]

class-map-name - Name of the class map. (Range: 1-32 characters)

match-any - sets the class map to match any packet.

Default Setting

match-any

Command Mode

Global Configuration

Command Usage

- ◆ First enter this command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the criteria for ingress traffic that will be classified under this class map.
- ◆ One or more class maps can be assigned to a policy map ([page 505](#)). The policy map is then bound by a service policy to an interface ([page 509](#)). A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the **match** or **set** commands.

Example

This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class
Console(config-cmap)#match cos 3
Console(config-cmap)#
```

Related Commands

[show class-map \(510\)](#)

description This command specifies the description of a class map or policy map. Use the **no** form of the command to delete the description of the class map or policy map.

Syntax

description *string*

no description

string - Description of the class map or policy map. (Range: 1-64 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description "matches packets marked for DSCP service
value 3"
Console(config-cmap)#
```

match This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

Syntax

```
[no] match {access-list acl-name | cos cos | ip dscp dscp |  
ip precedence ip-precedence | ipv6 dscp dscp | vlan vlan}
```

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 ACLs and MAC ACLs.
(Range: 1-16 characters)

cos - A Class of Service value. (Range: 0-7)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

vlan - A VLAN. (Range:1-4094)

Default Setting

None

Command Mode

Class Map Configuration

Command Usage

- ◆ First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the fields within ingress packets that must match to qualify for this class map.
- ◆ If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- ◆ If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- ◆ If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- ◆ Up to 16 match entries can be included in a class map.

Example

This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd-class#1  
Console(config-cmap)#match ip dscp 3  
Console(config-cmap)#
```


This example creates a class map call “rd-class#2,” and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call “rd-class#3,” and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename This command redefines the name of a class map or policy map.

Syntax

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-32 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

policy-map This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

Syntax

[no] policy-map *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches the criteria defined in a class map.
- ◆ A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command.
- ◆ Create a Class Map (page 505) before assigning it to a Policy Map.

Example

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set** command to classify the service that incoming packets will receive.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#
```

class This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

Syntax

[no] class *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Policy Map Configuration

Command Usage

- ◆ Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** command and one of the **police** commands to specify the match criteria, where the:
 - **set cos** command sets the class of service value in matching packets. (This modifies packet priority in the VLAN tag.)
 - **police** commands define parameters such as the maximum throughput, burst rate, and response to non-conforming traffic.
- ◆ Up to 16 classes can be included in a policy map.

Example

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set cos** command to classify the service that incoming packets will receive.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#
```

police rate This command defines an enforcer for classified traffic based on the metered flow rate. Use the **no** form to remove a policer.

Syntax

[no] police rate *committed-rate*

committed-rate - Committed information rate in kilobits per second.
(Range: 16-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ You can configure up to 16 policers (i.e., class maps) for ingress ports.
- ◆ The *committed-rate* cannot exceed the configured interface speed.
- ◆ Policing is based on a token bucket, where bucket depth is the maximum burst before the bucket overflows, and the average rate tokens that are added to the bucket is by specified by the *committed-rate* option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.
- ◆ The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).

The token bucket C is initially full, that is, the token count $T_c(0) = BC$. Thereafter, the token count T_c is updated CIR times per second as follows:

- If T_c is less than BC, T_c is incremented by one, else
- T_c is not incremented.

When a packet of size B bytes arrives at time t, the following happens:

- If $T_c(t) - B \geq 0$, the packet is green and T_c is decremented by B down to the minimum value of 0,
- else the packet is red and T_c is not decremented.

Example

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set cos** command to classify the service that incoming packets will receive, and then uses the **police rate** command to limit the average bandwidth to 100,000 Kbps.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police rate 100000
Console(config-pmap-c)#
```

set cos This command modifies the class of service (CoS) value for a matching packet (as specified by the **match** command) in the packet’s VLAN tag. Use the **no** form to remove this setting.

Syntax

[no] set cos *cos-value*

cos-value - Class of Service value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ The **set cos** command is used to set the CoS value in the VLAN tag for matching packets.

Example

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set cos** command to classify the service that incoming packets will receive.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
Console(config-pmap-c)#
```

set ip dscp This command modifies the IP DSCP value in a matching packet (as specified by the match command). Use the no form to remove this traffic classification.

Syntax

[no] set ip dscp dscp

dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

The set ip dscp command is used to set the priority values in the packet's ToS field for matching packets.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the **set ip dscp** command to classify the service that incoming packets will receive, and then uses the police rate command to limit the average bandwidth to 100,000 Kbps.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police rate 100000
Console(config-pmap-c)#
```

service-policy This command applies a policy map defined by the **policy-map** command to the ingress side of a particular interface. Use the **no** form to remove this mapping.

Syntax

[no] service-policy input policy-map-name

input - Apply to the input traffic.

policy-map-name - Name of the policy map for this interface.
(Range: 1-32 characters)

Default Setting

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.
- ◆ If the Ethernet interface is a member of a port channel then the service-policy cannot be applied and a binding error will occur.

Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

show class-map This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map *[class-map-name]*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all class maps.

Command Mode

Privileged Exec

Example

```
Console#show class-map
Class Map match-any rd-class#1
Description:
  Match ip dscp 10
  Match access-list rd-access
  Match ip dscp 0

Class Map match-any rd-class#2
  Match ip precedence 5

Class Map match-any rd-class#3
  Match vlan 1

Console#
```

show policy-map This command displays the QoS policy maps which define classification criteria for ingress or egress traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

policy-map-name - Name of the policy map. (Range: 1-32 characters)

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all policy maps and all classes.

Command Mode

Privileged Exec

Example

```
Console#show policy-map
Policy Map rd-policy
Description:
  class rd-class
  set PHB 3
  class finance-class
  police rate 100 class rd-class
Policy Map rd-policy
  class rd-class
    set PHB 3
Console#
```

show policy-map interface This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface *interface* **input**

interface

unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-)

Command Mode

Privileged Exec

Example

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#show policy-map interface
Interface ethernet 1/2
  service-policy input policy-map
Interface ethernet 1/3
```

```
service-policy input policy-map
Interface ethernet 1/4
service-policy input policy-map
Interface ethernet 1/5
service-policy input policy-map
Console#
```

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to check for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.



Note: A single table maintains a maximum of 511 entries learned for both IGMP and MLD snooping.

Note: Only ASM (any-source multicast) mode is supported on IGMPv3 and MLDv2. SSM (source-specific multicast) on IGMPv3 and MLDv2 is **not supported**. If a client sends an SSM report to the switch, the client will not join the multicast group.

Table 107: Multicast Filtering Commands

Command Group	Function
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, enables proxy reporting, displays current snooping settings, and displays the multicast service and group members
Static Multicast Routing	Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs
IGMP Filtering and Throttling	Configures IGMP filtering and throttling
MLD Snooping	Configures multicast snooping for IPv6
MLD Filtering and Throttling	Configures MLD filtering and throttling for IPv6.

IGMP Snooping

This section describes commands used to configure IGMP snooping on the switch.

Table 108: IGMP Snooping Commands

Command	Function	Mode
<code>ip igmp snooping</code>	Enables IGMP snooping	GC
<code>ip igmp snooping proxy-reporting</code>	Enables IGMP Snooping with Proxy Reporting	GC
<code>ip igmp snooping querier</code>	Allows this device to act as the querier for IGMP snooping	GC
<code>ip igmp snooping router-alert-option-check</code>	Discards any IGMPv2/v3 packets that do not include the Router Alert option	GC
<code>ip igmp snooping router-port-expire-time</code>	Configures the querier timeout	GC
<code>ip igmp snooping tcn-flood</code>	Floods multicast traffic when a Spanning Tree topology change occurs	GC
<code>ip igmp snooping tcn-query-solicit</code>	Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs	GC
<code>ip igmp snooping unregistered-data-flood</code>	Floods unregistered multicast traffic into the attached VLAN	GC
<code>ip igmp snooping unsolicited-report-interval</code>	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
<code>ip igmp snooping version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>ip igmp snooping vlan general-query-suppression</code>	Suppresses general queries except for ports attached to downstream multicast hosts	GC
<code>ip igmp snooping vlan immediate-leave</code>	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	GC
<code>ip igmp snooping vlan last-memb-query-count</code>	Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members	GC
<code>ip igmp snooping vlan last-memb-query-intvl</code>	Configures the last-member-query interval	GC
<code>ip igmp snooping vlan mrd</code>	Sends multicast router solicitation messages	GC
<code>ip igmp snooping vlan proxy-address</code>	Configures a static address for proxy IGMP query and reporting	GC
<code>ip igmp snooping vlan proxy-reporting</code>	Enables IGMP Snooping with Proxy Reporting	GC
<code>ip igmp snooping vlan query-interval</code>	Configures the interval between sending IGMP general queries	GC
<code>ip igmp snooping vlan query-resp-intvl</code>	Configures the maximum time the system waits for a response to general queries	GC
<code>ip igmp snooping vlan static</code>	Adds an interface as a member of a multicast group	GC

Table 108: IGMP Snooping Commands (Continued)

Command	Function	Mode
<code>ip igmp snooping</code> <code>vlan version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping</code> <code>vlan version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>clear ip igmp snooping</code> <code>groups dynamic</code>	Clears multicast group information dynamically learned through IGMP snooping	PE
<code>clear ip igmp snooping</code> <code>statistics</code>	Clears IGMP snooping statistics	PE
<code>show ip igmp snooping</code>	Shows the IGMP snooping, proxy, and query configuration	PE
<code>show ip igmp snooping</code> <code>group</code>	Shows known multicast group, source, and host port mapping	PE
<code>show ip igmp snooping</code> <code>mrouter</code>	Shows multicast router ports	PE
<code>show ip igmp snooping</code> <code>statistics</code>	Shows IGMP snooping protocol statistics for the specified interface	PE

ip igmp snooping This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the **no** form to disable it.

Syntax

[no] ip igmp snooping [vlan *vlan-id*]
vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
- ◆ When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

Example

The following example enables IGMP snooping globally.

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

ip igmp snooping proxy-reporting This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

Syntax

[no] ip igmp snooping proxy-reporting

ip igmp snooping vlan *vlan-id* proxy-reporting {enable | disable}

no ip igmp snooping vlan *vlan-id* proxy-reporting

vlan-id - VLAN ID (Range: 1-4094)

enable - Enable on the specified VLAN.

disable - Disable on the specified VLAN.

Default Setting

Global: Disabled

VLAN: Based on global setting

Command Mode

Global Configuration

Command Usage

- ◆ When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.
- ◆ If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

Example

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

ip igmp snooping querier This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[no] ip igmp snooping querier

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

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

ip igmp snooping router-alert-option- check

This command discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the **no** form to ignore the Router Alert Option when receiving IGMP messages.

Syntax

[no] ip igmp snooping router-alert-option-check

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

Example

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

ip igmp snooping router-port- expire-time

This command configures the querier timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535;
Recommended Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the timeout to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

ip igmp snooping tcn-flood This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable flooding.

Syntax

[no] ip igmp snooping tcn-flood

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into “multicast flooding mode” for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.
- ◆ If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a timeout mechanism is used to delete all of the currently learned multicast channels.
- ◆ When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.

- ◆ By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.
- ◆ When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

Example

The following example enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

ip igmp snooping tcn-query-solicit

This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable this feature.

Syntax

[no] ip igmp snooping tcn-query-solicit

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it will also immediately issues an IGMP general query.
- ◆ The **ip igmp snooping tcn query-solicit** command can be used to send a query solicitation whenever it notices a topology change, even if the switch is not the root bridge in the spanning tree.

Example

The following example instructs the switch to issue an IGMP general query whenever it receives a spanning tree topology change notification.

```
Console(config)#ip igmp snooping tcn-query-solicit  
Console(config)#
```

ip igmp snooping unregistered-data- flood

This command floods unregistered multicast traffic into the attached VLAN. Use the **no** form to drop unregistered multicast traffic.

Syntax

[no] ip igmp snooping unregistered-data-flood

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

Example

```
Console(config)#ip igmp snooping unregistered-data-flood  
Console(config)#
```

ip igmp snooping unsolicited-report- interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the **no** form to restore the default value.

Syntax

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- ◆ This command only applies when proxy reporting is enabled (see [page 516](#)).

Example

```
Console(config)#ip igmp snooping unsolicited-report-interval 5
Console(config)#
```

ip igmp snooping version This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping [vlan *vlan-id*] version {1 | 2 | 3}

no ip igmp snooping [vlan *vlan-id*] version

vlan-id - VLAN ID (Range: 1-4094)

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

Default Setting

Global: IGMP Version 2

VLAN: Not configured, based on global setting

Command Mode

Global Configuration

Command Usage

- ◆ This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
- ◆ If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

Example

The following configures the global setting for IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping version-exclusive This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the **ip igmp snooping version** command. Use the **no** form to disable this feature.

Syntax

[no] ip igmp snooping [vlan *vlan-id*] version-exclusive

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Global: Disabled

VLAN: Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- ◆ When this function is disabled, the currently selected version is backward compatible (see the **ip igmp snooping version** command).

Example

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```

ip igmp snooping vlan general-query-suppression This command suppresses general queries except for ports attached to downstream multicast hosts. Use the **no** form to flood general queries to all ports except for the multicast router port.

Syntax

[no] ip igmp snooping vlan *vlan-id* general-query-suppression

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ By default, general query messages are flooded to all ports, except for the multicast router through which they are received.
- ◆ If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

Example

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

ip igmp snooping vlan immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* **immediate-leave** [**by-host-ip**]

no ip igmp snooping vlan *vlan-id* **immediate-leave**

vlan-id - VLAN ID (Range: 1-4094)

by-host-ip - Specifies that the member port will be deleted only when there are no hosts joining this group.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the timeout period. (The timeout for this release is defined by Last Member Query Interval (fixed at one second) * Robustness Variable (fixed at 2) as defined in RFC 2236.)
- ◆ If immediate-leave is used, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- ◆ If the "by-host-ip" option is used, the router/querier will not send out a group-specific query when an IGMPv2/v3 leave message is received. But will check if there are other hosts joining the multicast group. Only when all hosts on that port leave the group will the member port be deleted.

- ◆ This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

ip igmp snooping vlan last-memb-query- count

This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* **last-memb-query-count** *count*

no ip igmp snooping vlan *vlan-id* **last-memb-query-count**

vlan-id - VLAN ID (Range: 1-4094)

count - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

Default Setting

2

Command Mode

Global Configuration

Command Usage

This command will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled ([page 516](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

ip igmp snooping vlan last-memb-query-intvl This command configures the last-member-query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-intvl *interval*

no ip igmp snooping vlan *vlan-id* last-memb-query-intvl

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)

Default Setting

10 (1 second)

Command Mode

Global Configuration

Command Usage

- ◆ When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.
- ◆ A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.
- ◆ This command will take effect only if IGMP snooping proxy reporting is enabled ([page 516](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

ip igmp snooping vlan mrd This command enables sending of multicast router solicitation messages. Use the **no** form to disable these messages.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrd

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.
- ◆ Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router's start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the **no ip igmp snooping vlan mrd** command.
- ◆ This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

Example

This example disables sending of multicast router solicitation messages on VLAN 1.

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

ip igmp snooping vlan proxy-address

This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the **no** form to restore the default source address.

Syntax

ip igmp snooping vlan *vlan-id* **proxy-address** *source-address*

no ip igmp snooping vlan *vlan-id* **proxy-address**

vlan-id - VLAN ID (Range: 1-4094)

source-address - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

Default Setting

0.0.0.0

Command Mode

Global Configuration

Command Usage

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- ◆ If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- ◆ If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

Example

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

ip igmp snooping vlan query-interval This command configures the interval between sending IGMP general queries. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-interval *interval*

no ip igmp snooping vlan *vlan-id* query-interval

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval between sending IGMP general queries.
(Range: 2-31744 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

- ◆ An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.
- ◆ This command applies when the switch is serving as the querier ([page 516](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 516](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

ip igmp snooping vlan query-resp-intvl This command configures the maximum time the system waits for a response to general queries. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-resp-intvl *interval*

no ip igmp snooping vlan *vlan-id* query-resp-intvl

vlan-id - VLAN ID (Range: 1-4094)

interval - The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second)

Default Setting

100 (10 seconds)

Command Mode

Global Configuration

Command Usage

This command applies when the switch is serving as the querier ([page 516](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 516](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```

ip igmp snooping vlan static This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[no] ip igmp snooping vlan *vlan-id* static *ip-address* interface

vlan-id - VLAN ID (Range: 1-4094)

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Static multicast entries are never aged out.
- ◆ When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Example

The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.1 ethernet 1/5
Console(config)#
```

clear ip igmp snooping groups dynamic This command clears multicast group information dynamically learned through IGMP snooping.

Syntax

clear ip igmp snooping groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through IGMP snooping. Statically configured multicast address are not cleared.

Example

```
Console#clear ip igmp snooping groups dynamic
Console#
```

clear ip igmp snooping statistics This command clears IGMP snooping statistics.

Syntax

clear ip igmp snooping statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN identifier (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#clear ip igmp snooping statistics
Console#
```

show ip igmp snooping This command shows the IGMP snooping, proxy, and query configuration settings.

Syntax

show ip igmp snooping [vlan *vlan-id*]

vlan-id - VLAN ID (1-4094)

Command Mode

Privileged Exec

Command Usage

This command displays global and VLAN-specific IGMP configuration settings.

Example

The following shows the current IGMP snooping configuration:

```

Console#show ip igmp snooping
IGMP Snooping                : Enabled
Router Port Expire Time      : 300 s
Router Alert Check          : Disabled
Router Port Mode             : Forward
TCN Flood                    : Disabled
TCN Query Solicit           : Disabled
Unregistered Data Flood      : Disabled
Unsolicited Report Interval  : 400 s
Version Exclusive            : Disabled
Version                      : 2
Proxy Reporting              : Disabled
Querier                      : Disabled

VLAN 1:
-----
IGMP Snooping                : Enabled
IGMP Snooping Running Status : Inactive
Version                      : Using global Version (2)
Version Exclusive            : Using global status (Disabled)
Immediate Leave              : Disabled
Last Member Query Interval   : 10 (unit: 1/10s)
Last Member Query Count      : 2
General Query Suppression    : Disabled
Query Interval               : 125
Query Response Interval      : 100 (unit: 1/10s)
Proxy Query Address          : 0.0.0.0
Proxy Reporting              : Using global status (Disabled)
Multicast Router Discovery    : Disabled

VLAN Static Group   Port
-----
1      224.1.1.1     Eth 1/ 1
:
```

show ip igmp snooping group This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

Syntax

show ip igmp snooping group [**host-ip-addr** [*ip-address* | *interface*] | **igmpsnp** | **sort-by-port** [*ip-address* | *interface*] | **user** | **vlan** *vlan-id* [**user** | **igmpsnp**]]

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-26)

vlan *vlan-id* - VLAN ID (1-4094)

igmpsnp - Display only entries learned through IGMP snooping.

sort-by-port - Display entries sorted by port.

user - Display only the user-configured multicast entries.

vlan-id - VLAN ID (1-4094)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1.

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).
```

VLAN	Group	Port	Up time	Expire Count
1	224.1.1.1	Eth 1/ 1 (R)	00:00:00:37	2 (P)

```
Console#                               Eth 1/ 2 (M)                               0 (H)
```

show ip igmp snooping mrouter This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the ports in VLAN 1 which are attached to multicast routers.

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type      Expire
-----
1     Eth 1/4                Dynamic 0:4:28
1     Eth 1/10               Static
Console#
```

show ip igmp snooping statistics This command shows IGMP snooping protocol statistics for the specified interface.

Syntax

show ip igmp snooping statistics

{**input** [interface *interface*] |

output [interface *interface*] |

query [vlan *vlan-id*]}

input - Specifies to display statistics for messages received by the interface.

output - Specifies to display statistics for messages sent by the interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays IGMP snooping-related statistics.

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows IGMP protocol statistics input:

```
Console#show ip igmp snooping statistics input interface ethernet 1/1
Input Statistics:
Interface Report    Leave    G Query    G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23         11         4             10         5         14         5
Console#
```

Table 109: show ip igmp snooping statistics input - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of multicast groups active on this interface.

The following shows IGMP protocol statistics output:

```
Console#show ip igmp snooping statistics output interface ethernet 1/1
Output Statistics:
Interface Report    Leave    G Query    G(-S)-S Query Drop    Group
-----
Eth 1/ 1           12         0         1             0         0         0
Console#
```

Table 110: show ip igmp snooping statistics output - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.
Group	The number of multicast groups active on this interface.

The following shows IGMP query-related statistics for VLAN 1:

```

Console#show ip igmp snooping statistics query vlan 1
Other Querier           : None
Other Querier Expire    : 0 (m) : 0 (s)
Other Querier Uptime    : 0 (h) : 0 (m) : 0 (s)
Self Querier            : 192.168.2.12
Self Querier Expire     : 0 (m) : 0 (s)
Self Querier Uptime     : 0 (h) : 0 (m) : 0 (s)
General Query Received  : 0
General Query Sent      : 0
Specific Query Received : 0
Specific Query Sent     : 0
Warn Rate Limit        : 0 sec.
V1 Warning Count        : 0
V2 Warning Count        : 0
V3 Warning Count        : 0
Console#

```

Table 111: show ip igmp snooping statistics vlan query - display description

Field	Description
Other Querier	IP address of remote querier on this interface.
Other Querier Expire	Time after which remote querier is assumed to have expired.
Other Querier Uptime	Time remote querier has been up.
Self Querier	IP address of local querier on this interface.
Self Querier Expire	Time after which local querier is assumed to have expired.
Self Querier Uptime	Time local querier has been up.
General Query Received	The number of general queries received on this interface.
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of specific queries received on this interface.
Specific Query Sent	The number of specific queries sent from this interface.

Table 111: show ip igmp snooping statistics vlan query - display description

Field	Description
Warn Rate Limit	The rate at which received query messages of the wrong version type cause the Vx warning count to increment. Note that "0 sec" means that the Vx warning count is incremented for each wrong message version received.
V1 Warning Count	The number of times the query version received (Version 1) does not match the version configured for this interface.
V2 Warning Count	The number of times the query version received (Version 2) does not match the version configured for this interface.
V3 Warning Count	The number of times the query version received (Version 3) does not match the version configured for this interface.

Static Multicast Routing

This section describes commands used to configure static multicast routing on the switch.

Table 112: Static Multicast Interface Commands

Command	Function	Mode
<code>ip igmp snooping vlan mrouter</code>	Adds a multicast router port	GC
<code>show ip igmp snooping mrouter</code>	Shows multicast router ports	PE

ip igmp snooping vlan mrouter This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

- ◆ Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.
- ◆ IGMP Snooping must be enabled globally on the switch (using the `ip igmp snooping` command) before a multicast router port can take effect.

Example

The following shows how to configure port 10 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

IGMP Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 113: IGMP Filtering and Throttling Commands

Command	Function	Mode
<code>ip igmp filter</code>	Enables IGMP filtering and throttling on the switch	GC
<code>ip igmp profile</code>	Sets a profile number and enters IGMP filter profile configuration mode	GC
<code>permit, deny</code>	Sets a profile access mode to permit or deny	IPC
<code>range</code>	Specifies one or a range of multicast addresses for a profile	IPC
<code>ip igmp filter</code>	Assigns an IGMP filter profile to an interface	IC
<code>ip igmp max-groups</code>	Specifies an IGMP throttling number for an interface	IC
<code>ip igmp max-groups action</code>	Sets the IGMP throttling action for an interface	IC
<code>ip igmp query-drop</code>	Drops any received IGMP query packets	IC
<code>show ip igmp filter</code>	Displays the IGMP filtering status	PE
<code>show ip igmp profile</code>	Displays IGMP profiles and settings	PE
<code>show ip igmp query-drop</code>	Shows if the interface is configured to drop IGMP query packets	PE
<code>show ip igmp throttle interface</code>	Displays the IGMP throttling setting for interfaces	PE

ip igmp filter This command globally enables IGMP filtering and throttling on the switch. Use the **(Global Configuration)** **no** form to disable the feature.

Syntax

[no] ip igmp filter

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- ◆ IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

Example

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

ip igmp profile This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[no] ip igmp profile profile-number

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can

be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny This command sets the access mode for an IGMP filter profile.

Syntax

{permit | deny}

Default Setting

Deny

Command Mode

IGMP Profile Configuration

Command Usage

- ◆ Each profile has only one access mode; either permit or deny.
- ◆ When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[no] range *low-ip-address* [*high-ip-address*]

low-ip-address - A valid IP address of a multicast group or start of a group range.

high-ip-address - A valid IP address for the end of a multicast group range.

Default Setting

None

Command Mode

IGMP Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration) This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

ip igmp filter *profile-number*

no ip igmp filter

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- ◆ The IGMP filtering profile must first be created with the [ip igmp profile](#) command before being able to assign it to an interface.
- ◆ Only one profile can be assigned to an interface.
- ◆ A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

Syntax

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-511)

Default Setting

511

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace” (see the [ip igmp max-groups action](#) command). If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- ◆ IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action This command sets the IGMP throttling action for an interface on the switch.

Syntax

ip igmp max-groups action {**deny** | **replace**}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

Default Setting

Deny

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

ip igmp query-drop This command drops any received IGMP query packets. Use the no form to restore the default setting.

Syntax

[no] ip igmp query-drop [vlan *vlan id*]

vlan - specifies to drop IGMP query packets received on the specified VLAN

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

show ip igmp filter This command displays the global and interface settings for IGMP filtering.

Syntax

show ip igmp filter [**interface** *interface*]
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-10/28)
port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp filter
IGMP Filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
-----
IGMP Profile 19
Deny
Range 239.1.1.1 239.1.1.1
Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile This command displays IGMP filtering profiles created on the switch.

Syntax

show ip igmp profile [*profile-number*]
profile-number - An existing IGMP filter profile number.
(Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp profile
IGMP Profile 19
Deny
```

```
Range 224.1.1.1      228.1.1.1
IGMP Profile 34
Deny
Range 229.1.1.1      235.255.255.254
Console#show ip igmp profile 19
IGMP Profile 19
Deny
Range 224.1.1.1      228.1.1.1
Console#
```

show ip igmp query-drop This command shows if the specified interface is configured to drop IGMP query packets.

Syntax

show ip igmp query-drop [**interface** *[interface]*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```


show ip igmp throttle interface This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-10/28)
port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
                Status : FALSE
                Action : Deny
        Max Multicast Groups : 1024
        Current Multicast Groups : 0

Console#
```

MLD Snooping

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Table 114: MLD Snooping Commands

Command	Function	Mode
<code>ipv6 mld snooping</code>	Enables MLD Snooping globally	GC
<code>ipv6 mld snooping proxy-reporting</code>	Enables MLD Snooping with Proxy Reporting	GC
<code>ipv6 mld snooping querier</code>	Allows the switch to act as the querier for MLD snooping	GC
<code>ipv6 mld snooping query-interval</code>	Configures the interval between sending MLD general query messages	GC
<code>ipv6 mld snooping query-max-response-time</code>	Configures the maximum response time for a general queries	GC
<code>ipv6 mld snooping robustness</code>	Configures the robustness variable	GC
<code>ipv6 mld snooping router-port-expire-time</code>	Configures the router port expire time	GC
<code>ipv6 mld snooping unknown-multicast mode</code>	Sets an action for unknown multicast packets	GC
<code>ipv6 mld snooping unsolicited-report-interval</code>	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
<code>ipv6 mld snooping version</code>	Configures the MLD Snooping version	GC
<code>ipv6 mld snooping vlan immediate-leave</code>	Removes a member port of an IPv6 multicast service if a leave packet is received at that port and MLD immediate-leave is enabled for the parent VLAN	GC
<code>ipv6 mld snooping vlan mrouter</code>	Adds an IPv6 multicast router port	GC
<code>ipv6 mld snooping vlan static</code>	Adds an interface as a member of a multicast group	GC
<code>clear ipv6 mld snooping groups dynamic</code>	Clears multicast group information dynamically learned through MLD snooping	PE

Table 114: MLD Snooping Commands (Continued)

Command	Function	Mode
<code>clear ipv6 mld snooping statistics</code>	Clears MLD snooping statistics	PE
<code>show ipv6 mld snooping</code>	Displays MLD Snooping configuration	PE
<code>show ipv6 mld snooping group</code>	Displays the learned multicast groups, source and host port mappings.	PE
<code>show ipv6 mld snooping mrouter</code>	Displays the information of multicast router ports	PE
<code>show ipv6 mld snooping statistics</code>	Shows IGMP snooping protocol statistics for the specified interface	PE

ipv6 mld snooping This command enables MLD Snooping globally on the switch. Use the **no** form to disable MLD Snooping.

Syntax

[no] ipv6 mld snooping

Default Setting

Disabled

Command Mode

Global Configuration

Example

The following example enables MLD Snooping:

```
Console(config)#ipv6 mld snooping
Console(config)#
```

ipv6 mld snooping proxy-reporting This command enables MLD Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

Syntax

[no] ipv6 mld snooping proxy-reporting

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When proxy reporting is enabled with this command, reports received from downstream hosts are summarized and used to build internal membership states. Proxy-reporting devices may use the IPv6 address configured on this VLAN or Source IP address from received report message as source address when forwarding any summarized reports upstream.

Example

```
Console(config)#ipv6 mld snooping proxy-reporting
Console(config)#
```

ipv6 mld snooping querier This command allows the switch to act as the querier for MLDv2 snooping. Use the no form to disable this feature.

Syntax

[no] ipv6 mld snooping querier

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.
- ◆ An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses its own IPv6 address as the query source address.
- ◆ The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

Example

```
Console(config)#ipv6 mld snooping querier
Console(config)#
```

ipv6 mld snooping query-interval This command configures the interval between sending MLD general queries. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

interval - The interval between sending MLD general queries.
(Range: 60-125 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

- ◆ This command applies when the switch is serving as the querier.
- ◆ An MLD general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

Example

```
Console(config)#ipv6 mld snooping query-interval 150
Console(config)#
```

ipv6 mld snooping query-max-response-time This command configures the maximum response time advertised in MLD general queries. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

seconds - The maximum response time allowed for MLD general queries.
(Range: 5-25 seconds)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

This command controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

Example

```
Console(config)#ipv6 mld snooping query-max-response-time 15
Console(config)#
```

ipv6 mld snooping robustness This command configures the MLD Snooping robustness variable. Use the **no** form to restore the default value.

Syntax

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)

Default Setting

2

Command Mode

Global Configuration

Command Usage

A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

Example

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port-expire-time This command configures the MLD query timeout. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port.
(Range: 300-500 seconds)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

Example

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

ipv6 mld snooping unknown-multicast mode

This command sets the action for dealing with unknown multicast packets. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping unknown-multicast mode {flood | to-router-port}

no ipv6 mld snooping unknown-multicast mode

flood - Floods the unknown multicast data packets to all ports.

to-router-port - Forwards the unknown multicast data packets to router ports.

Default Setting

to-router-port

Command Mode

Global Configuration

Command Usage

- ◆ When set to “flood,” any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.
- ◆ When set to “router-port,” any received IPv6 multicast packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

Example

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

ipv6 mld snooping unsolicited-report-interval This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the **no** form to restore the default value.

Syntax

ipv6 mld snooping unsolicited-report-interval *seconds*

no ipv6 mld snooping unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports.
(Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- ◆ This command only applies when proxy reporting is enabled (see [page 547](#)).

Example

```
Console(config)#ipv6 mld snooping unsolicited-report-interval 5
Console(config)#
```

ipv6 mld snooping version This command configures the MLD snooping version.

Syntax

ipv6 mld snooping version {1 | 2}

1 - MLD version 1.

2 - MLD version 2.

Default Setting

Version 2

Command Mode

Global Configuration

Example

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```


**ipv6 mld snooping
vlan immediate-leave**

This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* immediate-leave [by-host-ip]

vlan-id - A VLAN identification number. (Range: 1-4094)

by-host-ip - specifies to wait to delete the member port until all hosts have left the group.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.
- ◆ If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

Example

The following shows how to enable MLD immediate leave.

```
Console(config)#ipv6 mld snooping immediate-leave
Console(config)#
```

**ipv6 mld snooping
vlan mrouter**

This command statically configures an IPv6 multicast router port. Use the **no** form to remove the configuration.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 1 as a multicast router port within VLAN 1:

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

ipv6 mld snooping This command adds a port to an IPv6 multicast group. Use the **no** form to remove
vlan static the port.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* **static** *ipv6-address interface*

vlan - VLAN ID (Range: 1-4094)

ipv6-address - An IPv6 address of a multicast group. (Format: X:X:X:X::X)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ipv6 mld snooping vlan 1 static ff05:0:1:2:3:4:5:6 ethernet
1/6
Console(config)#
```

clear ipv6 mld snooping groups dynamic This command clears multicast group information dynamically learned through MLD snooping.

Syntax

clear ipv6 mld snooping groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through MLD snooping. Statically configured multicast address are not cleared.

Example

```
Console#clear ipv6 mld snooping groups dynamic
Console#
```

clear ipv6 mld snooping statistics This command clears MLD snooping statistics.

Syntax

clear ipv6 mld snooping statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN identifier (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#clear ipv6 mld snooping statistics
Console#
```

show ipv6 mld snooping This command shows the current MLD Snooping configuration.

Syntax

show ipv6 mld snooping [vlan [vlan-id]]

vlan-id - VLAN ID (1-4094)

Command Mode

Privileged Exec

Command Usage

This command displays global and VLAN-specific MLD snooping configuration settings.

Example

The following shows MLD Snooping configuration information

```
Console#show ipv6 mld snooping
Service Status           : Disabled
Proxy Reporting          : Disabled
Querier Status           : Disabled
Robustness               : 2
Query Interval           : 125 sec
Query Max Response Time  : 10 sec
Router Port Expiry Time  : 300 sec
Unsolicited Report Interval : 400 sec
Immediate Leave          : Disabled on all VLAN
Immediate Leave By Host  : Disabled on all VLAN
Unknown Flood Behavior   : To Router Port
MLD Snooping Version     : Version 2

VLAN Group IPv6 Address                                     Port
-----
1          ff05:0:1:2:3:4:5:6 Eth 1/1

Console#show ipv6 mld snooping vlan
VLAN 1
Immediate Leave          : Disabled
Unknown Flood Behavior   : To Router Port
Console#
```

show ipv6 mld snooping group This command shows known multicast groups, member ports, and the means by which each group was learned.

Syntax

show ipv6 mld snooping group [X:X:X:X::X | host-ip-addr [interface interface] | sort-by-port [interface interface] | source-list {X:X:X:X::X | vlan interface}]

X:X:X:X::X - Display the MLD information for the specified MLD group address.

host-ip-addr - Displays the VLANs and Group Host Addresses for the specified Ethernet port or port-channel.

sort-by-port - Similar to the `host-ip-addr` parameter but sorts the output by VLAN and the IP address.

source-list - Displays the MLD groups with their Source IP address.

vlan - Specifies the VLAN to show the MLD group information for.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

Command Mode

Privileged Exec

Example

The following shows MLD Snooping group configuration information:

```
Console#show ipv6 mld snooping group

Total Entries 3, limit 255

VLAN Multicast IPv6 Address          Member Port Type
-----
  1              FF02::01:01:01:01 Eth 1/1    MLD Snooping
  1              FF02::01:01:01:02 Eth 1/1    Multicast Data
  1              FF02::01:01:01:02 Eth 1/1    User

Console#
```

The following shows MLD Snooping group configuration information when the `host-ip-addr` parameter is used with the command:

```
Console#show ipv6 mld snooping group host-ip-addr ethernet 1/22
Port      VLAN Group
          Host
-----
Eth 1/22  1 ff02::fb
           fe80::f0a3:ea46:d9f2:90d5
Eth 1/22  1 ff02::1:fff2:90d5
           fe80::f0a3:ea46:d9f2:90d5
Eth 1/22  1 ff12::1:3

Console#
```

The following shows MLD Snooping group configuration information when the `sort-by-port` parameter is used with the command:

```

Console#show ipv6 mld snooping group sort-by-port ethernet 1/22

Expire: H:M:S; Uptime: H:M:S; T: Dynamic/Static; Q: Unreply query
Port      VLAN  Group                               Expire Uptime    T  Q
-----
Eth 1/22   1  ff02::fb                           2:28   0:1:59      D  0
Eth 1/22   1  ff02::1:fff2:90d5                  2:20   0:1:59      D  0
Eth 1/22   1  ff12::1:3                          2:23   0:1:56      D  0
Eth 1/22   1  ff17::101                          2:22   0:1:57      D  0
Eth 1/22   2  ff12::1:3                          2:54   0:1:25      D  0
Eth 1/22   2  ff17::101                          2:53   0:1:26      D  0

Port      VLAN  Group
Host
-----
Eth 1/22   1  ff02::fb
fe80::f0a3:ea46:d9f2:90d5
Eth 1/22   1  ff02::1:fff2:90d5
fe80::f0a3:ea46:d9f2:90d5
Eth 1/22   1  ff12::1:3

Console#

```

The following shows MLD Snooping group configuration information when the **vlan** parameter is used with the command:

```

Console#show ipv6 mld snooping group vlan 2

VLAN Multicast IPv6 Address          Member Port      Type
-----
2      ff12::1:3  Eth 1/22 (M)    MLD Snooping
2      ff17::101 Eth 1/22 (M)    MLD Snooping

Console#

```

The following shows MLD Snooping group configuration information when the **source-list** parameter is used with the command:

```

Console#show ipv6 mld snooping group source-list

VLAN ID          : 1
Multicast IPv6 Address : FF02::01:01:01:01
Member Port      : Eth 1/1
MLD Snooping     : Multicast Data
Filter Mode      : Include
(if exclude filter mode)
Filter Timer Elapse : 10 sec.
Request List      : ::01:02:03:04, ::01:02:03:05, ::01:02:03:06,
                  ::01:02:03:07
Exclude List      : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                  ::02:02:03:07
(if include filter mode)
Include List      : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                  ::02:02:03:06

Option:
Filter Mode: Include, Exclude

```

Console#

show ipv6 mld snooping mrouter This command shows MLD Snooping multicast router information.

Syntax

show ipv6 mld snooping mrouter [vlan *vlan-id*]

vlan-id - A VLAN identification number. (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 mld snooping mrouter
VLAN Multicast Router Port Type      Expire
-----
  1 Eth 1/ 2                      Static
Console#show ipv6 mld snooping mrouter vlan 1
VLAN Multicast Router Port Type      Expire
-----
  1 Eth 1/ 2                      Static
Console#
```

show ipv6 mld snooping statistics This command shows MLD snooping protocol statistics for the specified interface.

Syntax

show ipv6 mld snooping statistics

**{input [interface *interface*] |
output [interface *interface*] |
query [vlan *vlan-id*] |
summary interface *interface*}**

input - See [Table 115](#)

output - See [Table 116](#)

query - See [Table 117](#)

summary - See [Table 118](#)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MLD snooping query-related statistics.

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows MLD snooping input-related message statistics:

```
Console#show ipv6 mld snooping statistics input interface ethernet 1/1
Input Statistics:
Interface Report   Leave    G Query  G(-S)-S Query Drop      Join Succ Group
-----
Eth 1/ 1          4        0        0          0        0        0        2
Console#
```

Table 115: show ipv6 MLD snooping statistics input - display description

Field	Description
Interface	The unit/port or VLAN interface.
Report	The number of MLD membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MLD group report received.
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MLD groups active on this interface.

The following shows MLD snooping output-related message statistics:

```
Console#show ipv6 mld snooping statistics output interface ethernet 1/1
Output Statistics:
Interface Report   Leave    G Query  G(-S)-S Query Drop      Group
-----
Eth 1/ 1          0        0        5          0        0        2
Console#
```


Table 116: show ipv6 mld snooping statistics output - display description

Field	Description
Interface	The unit/port or VLAN interface.
Report	The number of MLD membership reports transmitted from this interface.
Leave	The number of leave messages transmitted from this interface.
G Query	The number of general query messages transmitted from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages transmitted from this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MLD group report received.
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MLD groups active on this interface.

The following shows MLD snooping query-related message statistics:

```

Console#show ipv6 mld snooping statistics query vlan 1
  Other Querier Address      : None
  Other Querier Expire      : 0 (m) : 0 (s)
  Other Querier Uptime      : 0 (h) : 0 (m) : 0 (s)
  Self Querier Address      : ::
  Self Querier Expire Time  : 1 (m) : 49 (s)
  Self Querier UpTime      : 0 (h) : 9 (m) : 6 (s)
  General Query Received    : 0
  General Query Sent       : 6
  Specific Query Received   : 0
  Specific Query Sent      : 0
Console#

```

Table 117: show ipv6 mld snooping statistics query - display description

Field	Description
Other Querier Address	IP address of remote querier on this interface.
Other Querier Expire	Time after which remote querier is assumed to have expired.
Other Querier Uptime	Time remote querier has been up.
Self Querier	IP address of local querier on this interface.
Self Querier Expire	Time after which local querier is assumed to have expired.
Self Querier Uptime	Time local querier has been up.
General Query Received	The number of general queries received on this interface.
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of group specific queries received on this interface.
Specific Query Sent	The number of group specific queries sent from this interface.

The following shows MLD snooping summary statistics:

```

Console#show ipv6 mld snooping statistics summary interface e 1/1
Number of Groups: 1
Querier:           :
Transmit           :
  General          : 6
  Group Specific: 0
Recieved           :
  General          : 0
  Group Specific: 0
Report & Leave:    :
Transmit           :
  Report           : 0
  Leave           : 0
Recieved           :
  Report           : 4
  Leave           : 0
  join Success     : 0
  Filter Drop      : 0
  Source Port Drop: 0
  Others Drop      : 0

Console#show ipv6 mld snooping statistics summary interface vlan 1
Number of Groups: 1
Querier:           :
  Other Querier    : None
Other Uptime       : 0(h):0(m):0(s)
Other Expire       : 0(m):0(s)
Self Addr          : None
Self Expire        : 2(m): 3(s)
Self Uptime        : 0(h):10(m):58(s)
Transmit           :
  General          : 7
  Group Specific: 0
Recieved           :
  General          : 0
  Group Specific: 0
Report & Leave:    :
Host Addr          : None
Unsolicit Expire   : 0 sec
Transmit           :
  Report           : 0
  Leave           : 0
Recieved           :
  Report           : 4
  Leave           : 0
  join Success     : 0
  Filter Drop      : 0
  Source Port Drop: 0
  Others Drop      : 0

Console#

```

Table 118: show ipv6 MLD snooping statistics summary - display description

Field	Description
Number of Groups	Number of active MLD groups active on the specified interface.
<i>Physical Interface (Port/Trunk)</i>	
<i>Querier:</i>	
<i>Transmit</i>	
General	The number of general queries sent from this interface.
Group Specific	The number of group specific queries sent from this interface.
<i>Recieved</i>	
General	The number of general queries received on this interface.
Group Specific	The number of group specific queries received on this interface.
<i>Report & Leave</i>	
<i>Transmit</i>	
Report	The number of MLD membership reports sent from this interface.

Table 118: show ipv6 MLD snooping statistics summary - display description

Field	Description
Leave	The number of leave messages sent from this interface.
<i>Recieved</i>	
Report	The number of MLD membership reports received on this interface.
Leave	The number of leave messages received on this interface.
Join Success	The number of times a multicast group was successfully joined.
Filter Drop	The number of messages dropped by an MLD filtering profile.
Source Port Drop	The number of dropped messages that are received on MVR source port or mrouter port.
Others Drop	The number of received invalid messages.
<i>Logical Interface (VLAN)</i>	The following additional parameters are included for a VLAN interface
<i>Querier:</i>	
Other Querier	IPv6 address of remote querier on this interface.
Other Uptime	Time remote querier has been up.
Other Expire	Time after which remote querier is assumed to have expired.
Self Addr	IPv6 address of local querier on this interface.
Self Expire	Time after which local querier is assumed to have expired.
Self Uptime	Time local querier has been up.
<i>Report & Leave</i>	
Host Addr	The link-local or global IPv6 address that is assigned on that VLAN.
Unsolicit Expire	The number of group leaves resulting from timeouts instead of explicit leave messages.

MLD Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

Table 119: MLD Filtering and Throttling Commands

Command	Function	Mode
<code>ipv6 mld filter</code>	Enables MLD filtering and throttling on the switch	GC
<code>ipv6 mld profile</code>	Sets a profile number and enters MLD filter profile configuration mode	GC
<code>permit, deny</code>	Sets a profile access mode to permit or deny	IPC
<code>range</code>	Specifies one or a range of multicast addresses for a profile	IPC

Table 119: MLD Filtering and Throttling Commands (Continued)

Command	Function	Mode
<code>ipv6 mld filter</code>	Assigns an MLD filter profile to an interface	IC
<code>ipv6 mld max-groups</code>	Specifies an M:D throttling number for an interface	IC
<code>ipv6 mld max-groups action</code>	Sets the MLD throttling action for an interface	IC
<code>ipv6 mld query-drop</code>	Drops any received MLD query packets	IC
<code>show ipv6 mld filter</code>	Displays the MLD filtering status	PE
<code>show ipv6 mld profile</code>	Displays MLD profiles and settings	PE
<code>show ipv6 mld query-drop</code>	Shows if the interface is configured to drop MLD query packets	PE
<code>show ipv6 mld throttle interface</code>	Displays the MLD throttling setting for interfaces	PE

ipv6 mld filter (Global Configuration) This command globally enables MLD filtering and throttling on the switch. Use the **no** form to disable the feature.

Syntax

[no] ipv6 mld filter

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.
- ◆ MLD filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- ◆ The MLD filtering feature operates in the same manner when MVR6 is used to forward multicast traffic.

Example

```
Console(config)#ipv6 mld filter
Console(config)#
```

Related Commands

[show ipv6 mld filter](#)

ipv6 mld profile This command creates an MLD filter profile number and enters MLD profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[no] ipv6 mld profile *profile-number*

profile-number - An MLD filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#
```

Related Commands

[show ipv6 mld profile](#)

permit, deny This command sets the access mode for an MLD filter profile.

Syntax

{permit | deny}

Default Setting

deny

Command Mode

MLD Profile Configuration

Command Usage

- ◆ Each profile has only one access mode; either permit or deny.

- ◆ When the access mode is set to permit, MLD join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, MLD join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#permit
Console(config-mld-profile)#
```

range This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[no] range *low-ipv6-address* [*high-ipv6-address*]

low-ipv6-address - A valid IPv6 address (X:X:X:X) of a multicast group or start of a group range.

high-ipv6-address - A valid IPv6 address (X:X:X:X) for the end of a multicast group range.

Default Setting

None

Command Mode

MLD Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config-mld-profile)#range ff01::0101 ff01::0202
Console(config-mld-profile)#
```

ipv6 mld filter (Interface Configuration) This command assigns an MLD filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

ipv6 mld filter *profile-number*

no ipv6 mld filter

profile-number - An MLD filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- ◆ The MLD filtering profile must first be created with the [ipv6 mld profile](#) command before being able to assign it to an interface.
- ◆ Only one profile can be assigned to an interface.
- ◆ A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld filter 19
Console(config-if)#
```

ipv6 mld max-groups This command configures the maximum number of MLD groups that an interface can join. Use the **no** form to restore the default setting.

Syntax

ipv6 mld max-groups *number*

no ipv6 mld max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-255)

Default Setting

255

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- ◆ MLD throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.
- ◆ If the maximum number of MLD groups is set to the default value, the running status of MLD throttling will change to false. This means that any configuration for MLD throttling will have no effect until the maximum number of MLD groups is configured to another value.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups 10
Console(config-if)#
```

ipv6 mld max-groups action This command sets the MLD throttling action for an interface on the switch.

Syntax

ipv6 mld max-groups action {deny | replace}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

Default Setting

Deny

Command Mode

Interface Configuration (Ethernet, Port-channel)

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups action replace
Console(config-if)#
```


ipv6 mld query-drop This command drops any received MLD query packets. Use the no form to restore the default setting.

Syntax

[no] ipv6 mld query-drop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld query-drop
Console(config-if)#
```

show ipv6 mld filter This command displays the global and interface settings for MLD filtering.

Syntax

show ipv6 mld filter [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ipv6 mld filter
MLD filter Enabled
Console#show ipv6 mld filter interface ethernet 1/3
Ethernet 1/3 information
-----
```

```
MLD Profile 19
Deny
Range ff01::101          ff01::faa
Console#
```

show ipv6 mld profile This command displays MLD filtering profiles created on the switch.

Syntax

show ipv6 mld profile [*profile-number*]

profile-number - An existing MLD filter profile number.
(Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ipv6 mld profile
MLD Profile 19
MLD Profile 50
Console#show ipv6 mld profile 19
MLD Profile 19
Deny
Range ff01::101          ff01::faa
Console#
```

show ipv6 mld query-drop This command shows if the specified interface is configured to drop MLD query packets.

Syntax

show ipv6 mld query-drop [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ipv6 mld query-drop
Ethernet 1/1: Enabled
Ethernet 1/2: Disabled
Ethernet 1/3: Disabled
Ethernet 1/4: Disabled
Ethernet 1/5: Disabled
Ethernet 1/6: Disabled
Ethernet 1/7: Disabled
Ethernet 1/8: Disabled
Ethernet 1/9: Disabled
Ethernet 1/10: Disabled
Console#show ipv6 mld query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ipv6 mld throttle interface This command displays the interface settings for MLD throttling.

Syntax

show ipv6 mld throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays information for all interfaces.

Example

```
Console#show ipv6 mld throttle interface ethernet 1/3
Eth 1/3 Information
  Status           : TRUE
  Action            : Replace
  Max Multicast Groups : 10
  Current Multicast Groups : 0

Console#
```

LLDP Commands

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 120: LLDP Commands

Command	Function	Mode
<code>lldp</code>	Enables LLDP globally on the switch	GC
<code>lldp holdtime-multiplier</code>	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC
<code>lldp med-fast-start-count</code>	Configures how many medFastStart packets are transmitted	GC
<code>lldp notification-interval</code>	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC
<code>lldp refresh-interval</code>	Configures the periodic transmit interval for LLDP advertisements	GC
<code>lldp reinit-delay</code>	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC
<code>lldp tx-delay</code>	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC
<code>lldp admin-status</code>	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC
<code>lldp basic-tlv management-ip-address</code>	Configures an LLDP-enabled port to advertise the management address for this device	IC
<code>lldp basic-tlv port-description</code>	Configures an LLDP-enabled port to advertise its port description	IC
<code>lldp basic-tlv system-capabilities</code>	Configures an LLDP-enabled port to advertise its system capabilities	IC

Table 120: LLDP Commands (Continued)

Command	Function	Mode
<code>lldp basic-tlv system-description</code>	Configures an LLDP-enabled port to advertise the system description	IC
<code>lldp basic-tlv system-name</code>	Configures an LLDP-enabled port to advertise its system name	IC
<code>lldp dot1-tlv proto-ident*</code>	Configures an LLDP-enabled port to advertise the supported protocols	IC
<code>lldp dot1-tlv proto-vid*</code>	Configures an LLDP-enabled port to advertise port-based protocol related VLAN information	IC
<code>lldp dot1-tlv pvid*</code>	Configures an LLDP-enabled port to advertise its default VLAN ID	IC
<code>lldp dot1-tlv vlan-name*</code>	Configures an LLDP-enabled port to advertise its VLAN name	IC
<code>lldp dot3-tlv link-agg</code>	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC
<code>lldp dot3-tlv mac-phy</code>	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC
<code>lldp dot3-tlv max-frame</code>	Configures an LLDP-enabled port to advertise its maximum frame size	IC
<code>lldp dot3-tlv poe</code>	Configures an LLDP-enabled port to advertise its Power-over-Ethernet capabilities	IC
<code>lldp med-location civic-addr</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-notification</code>	Enables the transmission of SNMP trap notifications about LLDP-MED changes	IC
<code>lldp med-tlv ext-poe</code>	Configures an LLDP-MED-enabled port to advertise its extended Power over Ethernet configuration and usage information	IC
<code>lldp med-tlv inventory</code>	Configures an LLDP-MED-enabled port to advertise its inventory identification details	IC
<code>lldp med-tlv location</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-tlv med-cap</code>	Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities	IC
<code>lldp med-tlv network-policy</code>	Configures an LLDP-MED-enabled port to advertise its network policy configuration	IC
<code>lldp notification</code>	Enables the transmission of SNMP trap notifications about LLDP changes	IC
<code>show lldp config</code>	Shows LLDP configuration settings for all ports	PE
<code>show lldp info local-device</code>	Shows LLDP global and interface-specific configuration settings for this device	PE
<code>show lldp info remote-device</code>	Shows LLDP global and interface-specific configuration settings for remote devices	PE
<code>show lldp info statistics</code>	Shows statistical counters for all LLDP-enabled interfaces	PE

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

Syntax

[no] lldp

Default Setting

Enabled

Command Mode

Global Configuration

Example

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

lldp holdtime-multiplier This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule:
minimum of ((Transmission Interval * Holdtime Multiplier), or 65536)

(Range: 2 - 10)

Default Setting

Holdtime multiplier: 4

TTL: $4 \times 30 = 120$ seconds

Command Mode

Global Configuration

Command Usage

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp med-fast-start-count This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. Use the **no** form to restore the default setting.

Syntax

lldp med-fast-start-count *packet-number*

no lldp med-fast-start-count

packet-number - Amount of packets. (Range: 1-10 packets; Default: 4 packets)

Default Setting

4 packets

Command Mode

Global Configuration

Command Usage

This parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Example

```
Console(config)#lldp med-fast-start-count 6
Console(config)#
```

lldp notification-interval This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

Syntax

lldp notification-interval *seconds*

no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

Default Setting

5 seconds

Command Mode

Global Configuration

Command Usage

- ◆ This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- ◆ Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#lldp notification-interval 30
Console(config)#
```

Ildp refresh-interval This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

Ildp refresh-interval *seconds*

no Ildp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

Default Setting

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

Ildp reinit-delay This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

Syntax

Ildp reinit-delay *seconds*

no Ildp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP.
(Range: 1 - 10 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Example

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

Syntax

lldp tx-delay *seconds*

no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

- ◆ The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.
- ◆ This attribute must comply with the following rule:
 $(4 * \text{tx-delay}) \leq \text{refresh-interval}$

Example

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

Syntax

lldp admin-status {rx-only | tx-only | tx-rx}

no lldp admin-status

rx-only - Only receive LLDP PDUs.

tx-only - Only transmit LLDP PDUs.

tx-rx - Both transmit and receive LLDP Protocol Data Units (PDUs).

Default Setting

tx-rx

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp basic-tlv management-ip-address This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv management-ip-address

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- ◆ The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

- ◆ Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- ◆ Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv port-description

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv system-capabilities

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv system-description

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv system-name

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the [hostname](#) command.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

Syntax**[no] lldp dot1-tlv proto-ident****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the protocols that are accessible through this interface.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid This command configures an LLDP-enabled port to advertise port-based protocol VLAN information. Use the **no** form to disable this feature.

Syntax**[no] lldp dot1-tlv proto-vid****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the port-based protocol VLANs configured on this interface (see [“Configuring Protocol-based VLANs” on page 476](#)).

Example

```

Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#

```

lldp dot1-tlv pvid This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

Syntax

[no] lldp dot1-tlv pvid

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the [switchport native vlan](#) command).

Example

```

Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#

```

lldp dot1-tlv vlan-name This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

Syntax

[no] lldp dot1-tlv vlan-name

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the name of all VLANs to which this interface has been assigned. See [“switchport allowed vlan” on page 465](#) and [“protocol-vlan protocol-group \(Configuring Interfaces\)” on page 477](#).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv link-agg

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv mac-phy

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv max-frame

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

Refer to [“Frame Size” on page 99](#) for information on configuring the maximum frame size for this switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe This command configures an LLDP-enabled port to advertise its Power-over-Ethernet (PoE) capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv poe

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command only applies to the PoE models.
- ◆ This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

lldp med-location civic-addr This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to restore the default settings.

Syntax

lldp med-location civic-addr [[**country** *country-code*] | [**what** *device-type*] | [*ca-type* *ca-value*]]

no lldp med-location civic-addr [[**country**] | [**what**] | [*ca-type*]]

country-code – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

device-type – The type of device to which the location applies.

0 – Location of DHCP server.

1 – Location of network element closest to client.

2 – Location of client.

ca-type – A one-octet descriptor of the data civic address value. (Range: 0-255)

ca-value – Description of a location. (Range: 1-32 characters)

Default Setting

Not advertised

No description

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Use this command without any keywords to advertise location identification details.

- ◆ Use the *ca-type* to advertise the physical location of the device, that is the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 121: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

- ◆ For the location options defined for *device-type*, normally option **2** is used to specify the location of the client device. In situations where the client device location is not known, **0** and **1** can be used, providing the client device is physically close to the DHCP server or network element.

Example

The following example enables advertising location identification details.

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 6 Exchange
Console(config-if)#lldp med-location civic-addr 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US

```

```
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#
```

lldp med-notification This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

Syntax

[no] lldp med-notification

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the [lldp notification-interval](#) command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the [snmp-server host](#) command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

lldp med-tlv ext-poe This command configures an LLDP-MED-enabled port to advertise and accept Extended Power-over-Ethernet configuration and usage information. Use the **no** form to disable this feature.

Syntax

[no] lldp med-tlv ext-poe

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command only applies to the PoE models.

This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv ext-poe
Console(config-if)#
```

lldp med-tlv inventory This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

Syntax**[no] lldp med-tlv inventory****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#
```

lldp med-tlv location This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

Syntax**[no] lldp med-tlv location****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises location identification details.

Example

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#

```

lldp med-tlv med-cap This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the **no** form to disable this feature.

Syntax**[no] lldp med-tlv med-cap****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

Example

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#

```

lldp med-tlv network-policy This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the **no** form to disable this feature.

Syntax**[no] lldp med-tlv network-policy****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

lldp notification This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

Syntax

[no] lldp notification

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the [lldp notification-interval](#) command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the [snmp-server host](#) command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

show lldp config This command shows LLDP configuration settings for all ports.

Syntax

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

The following example shows all basic LLDP parameters are enabled on Port 1.

```

Console#show lldp config
LLDP Global Configuration
  LLDP Enabled                : Yes
  LLDP Transmit Interval     : 30 seconds
  LLDP Hold Time Multiplier   : 4
  LLDP Delay Interval        : 2 seconds
  LLDP Re-initialization Delay : 2 seconds
  LLDP Notification Interval  : 5 seconds
  LLDP MED Fast Start Count   : 4

LLDP Port Configuration
Port      Admin Status Notification Enabled
-----
Eth 1/1   Tx-Rx          True
Eth 1/2   Tx-Rx          True
Eth 1/3   Tx-Rx          True
Eth 1/4   Tx-Rx          True
Eth 1/5   Tx-Rx          True
.
.
Console#show lldp config detail ethernet 1/1
LLDP Port Configuration Detail
Port                : Eth 1/1
Admin Status        : Tx-Rx
Notification Enabled : True
Basic TLVs Advertised : port-description
                    system-name
                    system-description
                    system-capabilities
                    management-ip-address
802.1 specific TLVs Advertised : port-vid
                    vlan-name
                    proto-vlan
                    proto-ident
802.3 specific TLVs Advertised : mac-phy
                    link-agg
                    max-frame
MED Notification Status : Enabled

```



```

MED Enabled TLVs Advertised      : med-cap
                                   network-policy
                                   location
                                   ext-poe
                                   inventory

MED Location Identification:
Location Data Format : Civic Address LCI
Civic Address Status : Enabled
Country Name       : US
What               : 2
CA-Type            : 1
CA-Value           : Alabama
CA-Type            : 2
CA-Value           : Tuscaloosa

Console#

```

show lldp info local-device This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```

Console#show lldp info local-device
LLDP Local Global Information
Chassis Type : MAC Address
Chassis ID   : 00-01-02-03-04-05
System Name  :
System Description : GEL-2861
System Capabilities Support : Bridge
System Capabilities Enabled : Bridge
Management Address : 192.168.0.101 (IPv4)

LLDP Port Information
Port  Port ID Type  Port ID  Port Description
-----
Eth 1/1  MAC Address  00-12-CF-DA-FC-E9 Ethernet Port on unit 0, port 1
Eth 1/2  MAC Address  00-12-CF-DA-FC-EA Ethernet Port on unit 0, port 2
Eth 1/3  MAC Address  00-12-CF-DA-FC-EB Ethernet Port on unit 0, port 3
Eth 1/4  MAC Address  00-12-CF-DA-FC-EC Ethernet Port on unit 0, port 4
.
.
.

```

```

Console#show lldp info local-device detail ethernet 1/1
LLDP Local Port Information Detail
Port          : Eth 1/1
Port ID Type  : MAC Address
Port ID       : 00-12-CF-DA-FC-E9
Port Description : Ethernet Port on unit 1, port 1
MED Capability : LLDP-MED Capabilities
                  Network Policy
                  Location Identification
                  Inventory

Console#

```

show lldp info remote-device This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [**detail** *interface*]

detail - Shows detailed information.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

Note that an IP phone or other end-node device which advertises LLDP-MED capabilities must be connected to the switch for information to be displayed in the "LLDP-MED Capability" and other related fields.

```

Console#show lldp info remote-device
LLDP Remote Devices Information
Interface Chassis ID      Port ID      System Name
-----
Eth 1/1    00-E0-0C-00-00-FD  00-E0-0C-00-01-02

Console#show lldp info remote-device detail ethernet 1/1
LLDP Remote Devices Information Detail
-----
Index          : 2
Chassis Type   : MAC Address
Chassis ID     : 70-72-CF-91-1C-B2
Port ID Type   : MAC Address
Port ID        : 70-72-CF-91-1C-B4
Time To Live   : 120 seconds
Port Description : Ethernet Port on unit 1, port 2
System Description : GEL-2861
System Capabilities : Bridge

```

```

Enabled Capabilities : Bridge

Management Address : 192.168.0.4 (IPv4)

Port VLAN ID : 1

Port and Protocol VLAN ID : supported, disabled

VLAN Name : VLAN    1 - DefaultVlan

Protocol Identity (Hex) : 88-CC

MAC/PHY Configuration/Status
Port Auto-neg Supported      : Yes
Port Auto-neg Enabled       : Yes
Port Auto-neg Advertised Cap (Hex) : 6C00
Port MAU Type                : 16

Power via MDI
Power Class                  : PSE
Power MDI Supported         : Yes
Power MDI Enabled           : Yes
Power Pair Controllable    : No
Power Pairs                  : Spare
Power Classification        : Class 1

Link Aggregation
Link Aggregation Capable   : Yes
Link Aggregation Enable    : No
Link Aggregation Port ID   : 0

Max Frame Size : 1522

Console#

```

The following example shows information which is displayed for end-node device which advertises LLDP-MED TLVs.

```

...
LLDP-MED Capability :
  Device Class      : Network Connectivity
  Supported Capabilities : LLDP-MED Capabilities
                        Network Policy
                        Location Identification
                        Extended Power via MDI - PSE
                        Inventory
  Current Capabilities : LLDP-MED Capabilities
                        Location Identification
                        Extended Power via MDI - PSE
                        Inventory

Location Identification :
  Location Data Format   : Civic Address LCI
  Country Name          : TW
  What                  : 2
Extended Power via MDI :
  Power Type            : PSE
  Power Source          : Unknown
  Power Priority         : Unknown
  Power Value           : 0 Watts
Inventory               :
  Hardware Revision     : R0A
  Firmware Revision     : 1.2.6.0

```

```

Software Revision      : 1.2.6.0
Serial Number         : S123456
Manufacture Name      : Prye
Model Name            : VP101
Asset ID              : 340937
Console#

```

show lldp info statistics This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

Syntax

show lldp info statistics [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```

Console#show lldp info statistics
LLDP Global Statistics
Neighbor Entries List Last Updated : 485 seconds
New Neighbor Entries Count         : 2
Neighbor Entries Deleted Count     : 1
Neighbor Entries Dropped Count     : 0
Neighbor Entries Ageout Count      : 1

LLDP Port Statistics
Port      NumFramesRecvd NumFramesSent NumFramesDiscarded
-----
Eth 1/1   12             12             0
Eth 1/2   17             17             0
Eth 1/3    0             0             0
Eth 1/4    0             0             0
Eth 1/5    0             0             0
:
Console#show lldp info statistics detail ethernet 1/1
LLDP Port Statistics Detail
Port Name      : Eth 1/1
Frames Discarded : 0
Frames Invalid  : 0
Frames Received : 12
Frames Sent     : 12
TLVs Unrecognized : 0
TLVs Discarded  : 0
Neighbor Ageouts : 1
Console#

```

Domain Name Service Commands

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the `ip name-server` command and domain lookup is enabled with the `ip domain-lookup` command.

Table 122: Address Table Commands

Command	Function	Mode
<i>DNS</i>		
<code>ip domain-list</code>	Defines a list of default domain names for incomplete host names	GC
<code>ip domain-lookup</code>	Enables DNS-based host name-to-address translation	GC
<code>ip domain-name</code>	Defines a default domain name for incomplete host names	GC
<code>ip host</code>	Creates a static IPv4 host name-to-address mapping	GC
<code>ip name-server</code>	Specifies the address of one or more name servers to use for host name-to-address translation	GC
<code>ipv6 host</code>	Creates a static IPv6 host name-to-address mapping	GC
<code>clear dns cache</code>	Clears all entries from the DNS cache	PE
<code>clear host</code>	Deletes entries from the host name-to-address table	PE
<code>show dns</code>	Displays the configuration for DNS services	PE
<code>show dns cache</code>	Displays entries in the DNS cache	PE
<code>show hosts</code>	Displays the static host name-to-address mapping table	PE
<i>mDNS</i>		
<code>ip mdns</code>	Enables multicast DNS	GC
<code>show ip mdns</code>	Shows configuration state for multicast DNS	GC

DNS Commands

ip domain-list This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

Syntax

[no] ip domain-list *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Domain names are added to the end of the list one at a time.
- ◆ When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- ◆ If there is no domain list, the domain name specified with the [ip domain-name](#) command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS Disabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
Console#
```

Related Commands

[ip domain-name \(600\)](#)

ip domain-lookup This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[no] ip domain-lookup

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ At least one name server must be specified before DNS can be enabled.
- ◆ If one or more name servers are configured, but DNS is not yet enabled and the switch receives a DHCP packet containing a DNS field with a list of DNS servers, then the switch will automatically enable DNS host name-to-address translation.
- ◆ If all name servers are deleted, DNS will automatically be disabled.

Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

[ip domain-name \(600\)](#)

[ip name-server \(601\)](#)

ip domain-name This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

Syntax

ip domain-name *name*

no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
Name Server List:
Console#
```

Related Commands

[ip domain-list \(598\)](#)

[ip name-server \(601\)](#)

[ip domain-lookup \(599\)](#)

ip host This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

Syntax

[no] ip host *name address*

name - Name of an IPv4 host. (Range: 1-127 characters)

address - Corresponding IPv4 address.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Use the **no ip host** command to clear static entries, or the **clear host** command to clear dynamic entries.

Example

This example maps an IPv4 address to a host name.

```

Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type      IP Address      TTL    Domain
-----
    0    2 Address 192.168.1.55
Console#

```

ip name-server This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

[no] ip name-server *server-address1* [*server-address2* ...
server-address6]

server-address1 - IPv4 or IPv6 address of domain-name server.

server-address2 ... *server-address6* - IPv4 or IPv6 address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list.

```

Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp

```

```
sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

Related Commands

[ip domain-name \(600\)](#)

[ip domain-lookup \(599\)](#)

ipv6 host This command creates a static entry in the DNS table that maps a host name to an IPv6 address. Use the **no** form to remove an entry.

Syntax

[no] ipv6 host *name ipv6-address*

name - Name of an IPv6 host. (Range: 1-127 characters)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

No static entries

Command Mode

Global Configuration

Example

This example maps an IPv6 address to a host name.

```
Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts
No.  Flag Type      IP Address          TTL   Domain
-----
0    2 Address 192.168.1.55          rd5
1    2 Address 2001:DB8:1::12      rd6
Console#
```

clear dns cache This command clears all entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#clear dns cache
Console#show dns cache
No.      Flag      Type      IP Address      TTL      Host
-----
Console#
```

clear host This command deletes dynamic entries from the DNS table.

Syntax

clear host {*name* | *}

name - Name of the host. (Range: 1-127 characters)

* - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Use the **clear host** command to clear dynamic entries, or the **no ip host** command to clear static entries.

Example

This example clears all dynamic entries from the DNS table.

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

show dns This command displays the configuration of the DNS service.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
  DNS enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

show dns cache This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#show dns cache
No.      Flag    Type    IP Address      TTL    Host
-----
3        4 Host    209.131.36.158  115    www-real.wal.b.yahoo.com
4        4 CNAME   POINTER TO:3    115    www.yahoo.com
5        4 CNAME   POINTER TO:3    115    www.wal.b.yahoo.com
Console#
```

Table 123: show dns cache - display description

Field	Description
No.	The entry number for each resource record.
Flag	The flag is always "4" indicating a cache entry and therefore unreliable.
Type	This field includes "Host" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server.
Host	The host name associated with this record.

show hosts This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```

Console#show hosts
No.  Flag Type      IP Address          TTL  Host
-----
0    2  Address 192.168.1.55          rd5
1    2  Address 2001:DB8:1::12       rd6
3    4  Address 209.131.36.158       65  www-real.wa1.b.yahoo.com
4    4  CNAME   POINTER TO:3         65  www.yahoo.com
5    4  CNAME   POINTER TO:3         65  www.wa1.b.yahoo.com
Console#

```

Table 124: show hosts - display description

Field	Description
No.	The entry number for each resource record.
Flag	The field displays "2" for a static entry, or "4" for a dynamic entry stored in the cache.
Type	This field includes "Address" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server. This field is always blank for static entries.
Host	The host name associated with this record.

Multicast DNS Commands

ip mdns This command enables multicast DNS. Use the **no** form to disable this feature.

Syntax

[no] ip mdns

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

Use this command to enable multicast DNS host name-to-address mapping on the local network without the need for a dedicated DNS server. For more information on this command refer to the *Web Management Guide*.

Example

```
Console(config)#ip mdns
Console(config)#
```

show ip mdns This command displays the configuration state multicast DNS service.

Command Mode

Privileged Exec

Example

```
Console#show ip mdns
Multicast DNS Status : Enabled
Console#
```

DHCP Commands (IPv4 and IPv6)

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client and relay functions. Any VLAN interface on this switch can be configured to automatically obtain an IP address through DHCP. This switch can also be configured to relay DHCP client configuration requests to a DHCP server on another network.

Table 125: DHCP Commands

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IP address information
DHCP Relay (IPv4 and IPv6)	Relays DHCP requests from local hosts to a remote DHCP server

DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 126: DHCP Client Commands

Command	Function	Mode
<i>DHCP for IPv4</i>		
<code>ip dhcp dynamic-provision</code>	Enables dynamic provision via DHCP	GC
<code>ip dhcp client class-id</code>	Specifies the DHCP client identifier for an interface	IC
<code>ip dhcp restart client</code>	Submits a BOOTP or DHCP client request	PE
<code>show ip dhcp dynamic-provision</code>	Shows the status of dynamic provision via DHCP	PE
<i>DHCP for IPv6</i>		
<code>ipv6 dhcp client rapid-commit vlan</code>	Specifies the Rapid Commit option for DHCPv6 message exchange	GC
<code>ipv6 dhcp restart client vlan</code>	Submits a DHCPv6 client request	PE
<code>show ipv6 dhcp duuid</code>	Shows the DHCP Unique Identifier for this switch	PE
<code>show ipv6 dhcp vlan</code>	Shows DHCPv6 information for specified interface	PE

DHCP for IPv4

ip dhcp dynamic-provision This command enables dynamic provisioning via DHCP. Use the **no** form to disable this feature.

Syntax

[no] ip dhcp dynamic-provision

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

DHCPD is the daemon used by Linux to dynamically configure TCP/IP information for client systems. To support DHCP option 66/67, you have to add corresponding statements to the configuration file of DHCPD. Information on how to complete this process are described in [“Downloading a Configuration File and Other Parameters from a DHCP Server” on page 59](#).

The following are some alternative commands which can be added to the DHCPD to complete the dynamic provisioning process.

By default, the parameters for DHCP option 66/67 are not carried by the reply sent from the DHCP server. To ask for a DHCP reply with option 66/67, the client can inform the server that it is interested in option 66/67 by sending a DHCP request that includes a 'parameter request list' option. Besides this, the client can also send a DHCP request that includes a 'vendor class identifier' option to the server so that the DHCP server can identify the device, and determine what information should be given to requesting device.

The following are two additional sample configurations of the dhcpd.conf file for the server version dhcp-3.0.4rc1, you can choose either one of them.

1. Define the conditions in subnet section:

```
shared-network Sample1 {
    subnet 192.168.1.0 netmask 255.255.255.0 {
        # option 55
        option dhcp-parameter-request-list 1,66,67;
        # option 66
        option tftp-server-name "192.168.1.1";
        # option 67
        option bootfile-name "dhcp_config.cfg ";
    }
}
```


2. Define the conditions in class section:

```

class "OPT66_67" { # for option 66/67
# option 124
    match if option vendor-class-identifier = "Level-1";
# option 55
    option dhcp-parameter-request-list 1,66,67;
# option 66
    option tftp-server-name "192.168.1.1";
# option 67
    option bootfile-name "dhcp_config.cfg";
}

shared-network Sample2 {
subnet 192.168.1.0 netmask 255.255.255.0 {
    }
    pool {
        allow members of "OPT66_67";
        range 192.168.1.10 192.168.1.20;
    }
}

```

Example

In the following example enables dhcp dynamic provisioning.

```

Console(config)#ip dhcp dynamic provisioning
Console(config)#

```

ip dhcp client class-id This command specifies the DHCP client vendor class identifier for the current interface. Use the **no** form to remove the class identifier from the DHCP packet.

Syntax

ip dhcp client class-id [*text text* | *hex hex*]

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters)

hex - A hexadecimal value. (Range: 1-64 characters)

Default Setting

Class identifier option enabled, using the model number as the string

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Use this command without any keyword to restore the default setting.

- ◆ This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- ◆ The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60, 66 and 67 statements can be added to the server daemon's configuration file.

Table 127: Options 60, 66 and 67 Statements

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

- ◆ By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides, the client request also includes a "vendor class identifier" set by the **ip dhcp client class-id** command that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 128: Options 55 and 124 Statements

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

- ◆ The server should reply with Option 66 attributes, including the TFTP server name and boot file name.
- ◆ Note that the vendor class identifier can be formatted in either text or hexadecimal using the **ip dhcp client class-id** command, but the format used by both the client and server must be the same.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

Related Commands

[ip dhcp restart client \(611\)](#)

ip dhcp restart client This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the [ip address](#) command.
- ◆ DHCP requires the server to reassign the client's last address if available.
- ◆ If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-00-00-00-01
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): GEL-2861
  DHCP Relay Server:
Console#
```

Related Commands

[ip address \(622\)](#)

show ip dhcp dynamic-provision This command shows the status of dynamic provision via DHCP.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp dynamic provisioning
Dynamic Provision via DHCP Status: Disabled
Console#
```

DHCP for IPv6

ipv6 dhcp client rapid-commit vlan This command specifies the Rapid Commit option for DHCPv6 message exchange for all DHCPv6 client requests submitted from the specified interface. Use the **no** form to disable this option.

Syntax

[no] ipv6 dhcp client rapid-commit vlan *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ DHCPv6 clients can obtain configuration parameters from a server through a normal four-message exchange (solicit, advertise, request, reply), or through a rapid two-message exchange (solicit, reply). The rapid-commit option must be enabled on both client and server for the two-message exchange to be used.
- ◆ This command allows two-message exchange method for prefix delegation. When enabled, DHCPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.
- ◆ If the rapid commit option has been enabled on the switch with this command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

Example

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

ipv6 dhcp restart client vlan This command submits a DHCPv6 client request.

Syntax

ipv6 dhcp restart client vlan *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ This command starts the DHCPv6 client process if it is not yet running by submitting requests for configuration information through the specified interface(s). When DHCPv6 is restarted, the switch may attempt to acquire an IP address prefix through stateful address auto-configuration. If the router advertisements have the “other stateful configuration” flag set, the switch may also attempt to acquire other non-address configuration information (such as a default gateway or DNS server) when DHCPv6 is restarted.

Prior to submitting a client request to a DHCPv6 server, the switch should be configured with a link-local address using the [ipv6 address autoconfig](#) command. The state of the Managed Address Configuration flag (M flag) and Other Stateful Configuration flag (O flag) received in Router Advertisement messages will determine the information this switch should attempt to acquire from the DHCPv6 server as described below.

- Both M and O flags are set to 1:

DHCPv6 is used for both address and other configuration settings.

This combination is known as DHCPv6 stateful, in which a DHCPv6 server assigns stateful addresses to IPv6 hosts.

- The M flag is set to 0, and the O flag is set to 1:

DHCPv6 is used only for other configuration settings.

Neighboring routers are configured to advertise non-link-local address prefixes from which IPv6 hosts derive stateless addresses.

This combination is known as DHCPv6 stateless, in which a DHCPv6 server does not assign stateful addresses to IPv6 hosts, but does assign stateless configuration settings.

- ◆ DHCPv6 clients build a list of servers by sending a solicit message and collecting advertised message replies. These servers are then ranked based on their advertised preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.
- ◆ If the rapid commit option has been enabled on the switch using the [ipv6 dhcp client rapid-commit vlan](#) command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

Example

The following command submits a client request on VLAN 1.

```
Console#ipv6 dhcp restart client vlan 1
Console#
```

Related Commands

[ipv6 address autoconfig \(636\)](#)

show ipv6 dhcp duid This command shows the DHCP Unique Identifier for this switch.

Command Mode

Privileged Exec

Command Usage

DHCPv6 clients and servers are identified by a DHCP Unique Identifier (DUID) included in the client identifier and server identifier options. Static or dynamic address prefixes may be assigned by a DHCPv6 server based on the client's DUID.

Example

```
Console#show ipv6 dhcp duid
DHCPv6 Unique Identifier (DUID): 0001-0001-4A8158B4-00E00C0000FD
Console#
```

show ipv6 dhcp vlan This command shows DHCPv6 information for the specified interface(s).

Syntax

show ipv6 dhcp vlan *vlan-list*

vlan-list - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Command Usage

Each allocation in the DHCPv6 server is identified by a DUID and an IAID. IAID means Interface Association Identifier, and is a binding between the interface and one or more IP addresses.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode, Rapid-Commit
IAID:                                C0000F0
```

```
List of known servers:
  Server address : FE80::250:FCFF:FEF9:A494
  DUID           : 0001-0001-48CFB0D5-F48F2A006801

  Server address : FE80::250:FCFF:FEF9:A405
  DUID           : 0001-0001-38CF5AB0-F48F2A003917
Console#
```

RELATED COMMANDS

[ipv6 address \(635\)](#)

DHCP Relay (IPv4 and IPv6)

This section describes commands used to configure the switch to relay DHCP (v4 and v6) requests from local hosts to a remote DHCP server.

Table 129: DHCP Relay Commands

Command	Function	Mode
<i>DHCP Relay for IPv4</i>		
ip dhcp relay server	Specifies DHCP server or relay server addresses	GC,IC
ip dhcp restart relay	Enables DHCP relay agent	PE
<i>DHCP Relay for IPv6</i>		
ipv6 dhcp relay destination	Specifies DHCP server or relay server destination addresses	GC,IC
ipv6 dhcp relay destination multicast	Specifies to relay DHCv6 messages using the multicast destination address	GC,IC
show ipv6 dhcp relay destination interface	Displays the DHCPv6 configured destinations	GC

ip dhcp relay server This command specifies the DHCP server or relay server addresses to use. Use the **no** form to clear all addresses or specify a single address to remove.

Syntax

[no] ip dhcp relay server *address1* [*address2* [*address3* ...]]

address - IP address of DHCP server. (Range: 1-5 addresses)

Default Setting

None

Command Mode

Global Configuration, Interface Configuration (VLAN)

Usage Guidelines

- ◆ DHCP relay service at the VLAN interface configuration level applies to DHCP client requests received on the specified VLAN.
- ◆ This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP client request, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.
- ◆ You must specify the IP address for at least one active DHCP server. Otherwise, the switch's DHCP relay agent will not be able to forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference.

If any of the specified DHCP server addresses are not located in the same network segment with this switch, use the [ip default-gateway](#) or [ipv6 default-gateway](#) command to specify the default router through which this switch can reach other IP subnetworks.
- ◆ To start DHCP relay service, enter the [ip dhcp restart relay](#) command.

Example

This example configures the switch to enable DHCP relay service for VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 192.168.10.19
Console(config-if)#
```

Related Commands

[ip dhcp restart relay \(616\)](#)

ip dhcp restart relay This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

Default Setting

Disabled

Command Mode

Privileged Exec

Command Usage

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch receives a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server

will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console#ip dhcp restart relay
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-00-E8-93-82-A0
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 10.1.0.254 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): GEL-2861
  DHCP Relay Server:
Console#
```

Related Commands

[ip dhcp relay server \(615\)](#)

ipv6 dhcp relay destination Use this command to enable IPv6 DHCP relay agent service and specify a DHCPv6 destination unicast addresses. Use the **no** form of the command to delete all DHCPv6 relay agent destinations or specify a single destination address to be removed.

Syntax

ipv6 dhcp relay destination *address1* [*address2* [*address3*...]]

no ipv6 dhcp relay destination [*address*]

address - IPv6 address of DHCPv6 server or relay agent (Range: 1-5 addresses)

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

A maximum of five DHCPv6 server or relay agent unicast addresses can be configured.

DHCP relay service is enabled on the VLAN when at least one Unicast or Multicast entry is configured.

Once an entry is entered using the command, the switch will listen on UDP port 547 for DHCPv6 messages from DHCPv6 clients and forward the messages to the configured destination address(es).

The layer 3 interface of the configured or destination VLAN must have its layer 3 interface enabled. (Adding an IPv6 or IP address to the VLAN interface will enable it.)

The relay agent is enabled if the command `show ipv6 dhcp relay destination interface` displays at least one entry for a configured VLAN. The relay agent is disabled if the command displays no entries.

Example

This example configures the switch to enable DHCPv6 relay agent service for VLAN 200 and sets a unicast destination IPv6 address.

```
Console(config)#interface vlan 200
Console(config-if)#ipv6 dhcp relay destination 2001:0db8:85a3::8a2e:0370:7334
Console(config-if)#
```

ipv6 dhcp relay destination multicast

This command will enable the DHCPv6 relay agent and forward DHCPv6 client messages to a multicast address. Use the no form of the command to delete all DHCPv6 relay agent multicast destinations or specify a single multicast destination address to be removed.

Syntax

ipv6 dhcp relay destination multicast {all | vlan *vlan-id*}

no ipv6 dhcp relay destination multicast {all | vlan *vlan-id*}

all - all configured VLANs

vlan *vlan-id* (Range: 1-4094)

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

Use this command if you do not know the Unicast destination address of the DHCPv6 servers or other relay agents. This command will relay DHCPv6 client messages to a DHCPv6 server or relay agent by forwarding the messages to the multicast address ALL_DHCP_SERVERS (FF05::1:3).

The command can be entered by either configuring a specific VLAN or using the "all" option to specify all configured VLANs on which the DHCPv6 client message

will be forwarded using the multicast address. Multiple specific VLANs can be entered by repeating the command for each specific VLAN.

Once an entry is entered using this command, the switch will listen on UDP port 547 for DHCPv6 messages from DHCPv6 clients. It will forward the client messages on all or specified VLANs using the multicast address as the destination.

The layer 3 interface of the configured or destination VLAN must have its layer 3 interface enabled. (Adding an IPv6 or IP address to the VLAN interface will enable it.)

The relay agent is enabled if the command `show ipv6 dhcp relay destination interface` displays at least one entry for a configured VLAN. The relay agent is disabled if the command displays no entries.

Example

In this example VLAN 600 is configured to forward client DHCPv6 messages out on all configured VLANs using the multicast address FF05::1:3.

```
Console(config)#interface vlan 600
Console(config-if)#ipv6 dhcp relay destination multicast all
Console(config-if)#
```

show ipv6 dhcp relay destination interface Use this command to show the DHCPv6 relay agent configuration.

Syntax

show ipv6 dhcp relay destination interface [vlan *vlan-id*]

vlan *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Privileged Exec.

Example

In this example the DHCPv6 relay agent destinations for all configured VLANs with DHCPv6 relay service enabled is shown. Note that the DHCPv6 relay service is disabled for VLANs 600, 610 and 620; no entries are displayed. DHCPv6 relay service is enabled on VLANs 1, 200 and 300.

```
Console#show ipv6 dhcp relay destination interface
DHCP relay destination :
VLAN 1 :
  Multicast : VLAN 100
VLAN 200 :
  Unicast   : 2001:db8:85a3::8a2e:370:7334
```

```
2001:db8:85a3::8a2e:370:7336
2001:db8:85a3::8a2e:470:7334
2001:db8:85a3::8a2e:470:7336
2001:db8:85a3::8a2e:570:7334
VLAN 300 :
  Multicast : VLAN 600
              VLAN 610
              VLAN 620
VLAN 600 :
VLAN 610 :
VLAN 620 :
Console(config)#
```

IP Interface Commands

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

Table 130: IP Interface Commands

Command Group	Function
IPv4 Interface	Configures an IPv4 address for the switch
IPv6 Interface	Configures an IPv6 address for the switch

IPv4 Interface

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

Table 131: IPv4 Interface Commands

Command Group	Function
Basic IPv4 Configuration	Configures the IP address for interfaces and the gateway router
ARP Configuration	Configures static, dynamic and proxy ARP service

Basic IPv4 Configuration This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 132: Basic IP Configuration Commands

Command	Function	Mode
<code>ip address</code>	Sets the IP address for the current interface	IC
<code>ip default-gateway</code>	Defines the default gateway through which this switch can reach other subnetworks	GC
<code>show ip interface</code>	Displays the IP settings for this device	PE
<code>show ip traffic</code>	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
<code>traceroute</code>	Shows the route packets take to the specified host	PE
<code>ping</code>	Sends ICMP echo request packets to another node on the network	NE, PE
<code>ip multicast-data-drop</code>	Drops all multicast data packets	IC
<code>show ip multicast-data-drop</code>	Shows if the interface is configured to drop multicast data packets	PE

ip address This command sets the IPv4 address for the currently selected VLAN interface. Use the **no** form to remove an IP address.

Syntax

ip address *{ip-address netmask [secondary]*
[default-gateway ip-address] | bootp | dhcp}

no ip address *[ip-address netmask [secondary] | dhcp]*

ip-address - IP address

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask can be either in the traditional format xxx.xxx.xxx.xxx or use classless format with the range /5 to /32. For example the subnet 255.255.224.0 would be /19.

secondary - Specifies a secondary IP address.

default-gateway - The default gateway. (Refer to the [ip default-gateway](#) command which provides the same function.)

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

Default Setting

192.168.2.10/24

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not accepted by the configuration program.
- ◆ An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router/switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.
- ◆ If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the [ip dhcp restart client](#) command to re-start broadcasting service requests, or reboot the switch.



Note: Each VLAN group can be assigned its own IP interface address. You can manage the switch via any of these IP addresses.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

This example assigns an IP address to VLAN 2 using a classless network mask.

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.2.2.1/24
Console(config-if)#
```

Related Commands

[ip dhcp restart client \(602\)](#)
[ip default-gateway \(624\)](#)
[ipv6 address \(635\)](#)

ip default-gateway This command specifies the default gateway for destinations not found in local routing tables. Use the **no** form to remove a default gateway.

Syntax

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No default gateway is established.

Command Mode

Global Configuration

Command Usage

- ◆ The default gateway can also be defined using the following Global configuration command: **ip route 0.0.0.0 0.0.0.0** *gateway-address*.
- ◆ Static routes can also be defined using the **ip route** command to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- ◆ A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address for a default gateway, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 192.168.0.1
Console(config)#
```

Related Commands

[ip address \(622\)](#)

[ip route \(660\)](#)

[ipv6 default-gateway \(634\)](#)

show ip interface This command displays the settings of an IPv4 interface.

Command Mode
Privileged Exec

Example

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-00-00-00-01
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  DHCP Client Vendor Class ID (text): GEL-2861
Console#
```

Related Commands

[ip address \(622\)](#)
[show ipv6 interface \(643\)](#)

show ip traffic This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode
Privileged Exec

Example

```
Console#show ip traffic
IP Statistics:
IP received
    7845 total received
        header errors
        unknown protocols
        address errors
        discards
    7845 delivers
        reassembly request datagrams
        reassembly succeeded
        reassembly failed
IP sent
    forwards datagrams
    9903 requests
        discards
        no routes
        generated fragments
        fragment succeeded
        fragment failed
ICMP Statistics:
ICMP received
    input
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
```

```
timestamp request messages
timestamp reply messages
source quench messages
address mask request messages
address mask reply messages

ICMP sent
output
errors
destination unreachable messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
redirect messages
timestamp request messages
timestamp reply messages
source quench messages
address mask request messages
address mask reply messages

UDP Statistics:
input
no port errors
other errors
output

TCP Statistics:
7841 input
input errors
9897 output

Console#
```

traceroute This command shows the route packets take to the specified destination.

Syntax

traceroute *host*

host - IP address or alias of the host.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **traceroute** command to determine the path taken to reach a specified destination.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all

devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

- ◆ If the target device does not respond or other errors are detected, the switch will indicate this by one of the following messages:
 - * - No Response
 - H - Host Unreachable
 - N - Network Unreachable
 - P - Protocol Unreachable
 - O -Other

Example

```

Console#traceroute 192.168.0.1
Press "ESC" to abort.
Traceroute to 192.168.0.99, 30 hops max, timeout is 3 seconds
Hop  Packet 1 Packet 2 Packet 3 IP Address
-----
 1      20 ms   <10 ms   <10 ms 192.168.0.99

Trace completed.
Console#

```

ping This command sends (IPv4) ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*] [**size** *size*]

host - IP address or alias of the host.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 32-512)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

count: 5

size: 32 bytes

Command Mode

Normal Exec, Privileged Exec

Command Usage

- ◆ Use the ping command to see if another site on the network can be reached.

- ◆ The following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- ◆ When pinging a host name, be sure the DNS server has been defined ([page 601](#)) and host name-to-address translation enabled ([page 599](#)). If necessary, local devices can also be specified in the DNS static host table ([page 600](#)).

Example

```
Console#ping 10.1.0.9
Press ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

[interface \(350\)](#)

ip multicast-data-drop This command configures an interface to drop all UDP multicast data packets. Use the **no** form to disable this feature.

Syntax

[no] ip multicast-data-drop

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can be used to stop multicast services using UDP packets from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

show ip multicast-data-drop This command shows if the specified interface is configured to drop multicast data packets.

Syntax

show ip multicast-data-drop [**interface** *[interface]*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10/28)

port-channel *channel-id* (Range: 1-24)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

ARP Configuration This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 133: Address Resolution Protocol Commands

Command	Function	Mode
<code>arp</code>	Adds a static entry in the ARP cache	GC
<code>ip proxy-arp</code>	Enables proxy ARP service	IC
<code>clear arp-cache</code>	Deletes all dynamic entries from the ARP cache	PE
<code>show arp</code>	Displays entries in the ARP cache	NE, PE

arp This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*

no arp *ip-address*

ip-address - IP address to map to a specified hardware address.

hardware-address - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting

No default entries

Command Mode

Global Configuration

Command Usage

- ◆ The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- ◆ The maximum number of static entries allowed in the ARP cache is 8.
- ◆ A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- ◆ Static entries will not be aged out nor deleted when power is reset. A static entry can only be removed through the configuration interface.

Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

[clear arp-cache \(632\)](#)

[show arp \(632\)](#)

ip proxy-arp This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

Syntax

[no] ip proxy-arp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.
- ◆ End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- ◆ Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Example

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

clear arp-cache This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode
Privileged Exec

Command Mode
The command only deletes dynamic entries in the ARP cache.

The maximum number of dynamic ARP cache entries is 48.

Example
This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Do you want to continue this operation (y/n)?
Console#
```

show arp This command displays entries in the Address Resolution Protocol (ARP) cache.

Command Mode
Normal Exec, Privileged Exec

Command Usage

- ◆ This command displays information about the ARP cache. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type “other” indicates local addresses for this router.
- ◆ Static entries are only displayed for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of a existing VLAN, and that VLAN is linked up.
- ◆ The maximum number of ARP entries is 64; which is limited to 8 static entries, 48 dynamic entries and 8 entries that are reserved for VLAN interfaces. For the GEL-1061 switch model, the table is shared with IPV6 ND, which may limit the total available entries for ARP.

Example
This example displays all entries in the ARP cache.

```
Console#show arp
```

IP Address	MAC Address	Type	Interface
192.168.1.1	00-11-3B-11-22-33	other	VLAN1
192.168.1.2	00-E0-4C-68-14-79	dynamic	VLAN1


```
145.30.20.23    09-50-40-30-20-10 dynamic  VLAN3
```

```
Total entry : 3
Console#
```

IPv6 Interface

This switch supports the following IPv6 interface commands.

Table 134: IPv6 Configuration Commands

Command	Function	Mode
<i>Interface Address Configuration and Utilities</i>		
<code>ipv6 default-gateway</code>	Sets an IPv6 default gateway for traffic with no known next hop	GC
<code>ipv6 address</code>	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC
<code>ipv6 address autoconfig</code>	Enables automatic configuration of IPv6 addresses on an interface and enables IPv6 on the interface	IC
<code>ipv6 address eui-64</code>	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC
<code>ipv6 address link-local</code>	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC
<code>ipv6 enable</code>	Enables IPv6 on an interface that has not been configured with an explicit IPv6 address	IC
<code>ipv6 mtu</code>	Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface	IC
<code>show ipv6 default-gateway</code>	Displays the current IPv6 default gateway	PE
<code>show ipv6 interface</code>	Displays the usability and configured settings for IPv6 interfaces	PE
<code>show ipv6 mtu</code>	Displays maximum transmission unit (MTU) information for IPv6 interfaces	PE
<code>show ipv6 traffic</code>	Displays statistics about IPv6 traffic	PE
<code>clear ipv6 traffic</code>	Resets IPv6 traffic counters	PE
<code>ping6</code>	Sends IPv6 ICMP echo request packets to another node on the network	PE
<code>traceroute6</code>	Shows the route packets take to the specified host	PE
<i>Neighbor Discovery</i>		
<code>ipv6 nd dad attempts</code>	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC
<code>ipv6 nd ns-interval</code>	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC
<code>ipv6 nd reachable-time</code>	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred	IC

Table 134: IPv6 Configuration Commands (Continued)

Command	Function	Mode
<code>clear ipv6 neighbors</code>	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE
<code>show ipv6 neighbors</code>	Displays information in the IPv6 neighbor discovery cache	PE

Interface Address Configuration and Utilities

ipv6 default-gateway This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the **no** form to remove a previously configured default gateway.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address - The IPv6 address of the default next hop router to use for destinations with no known next hop.

Default Setting

No default gateway is defined

Command Mode

Global Configuration

Command Usage

- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.
- ◆ An IPv6 default gateway should be defined if the destination has been assigned an IPv6 address that is located in a different IP segment.
- ◆ An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

Example

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1
Console(config)#
```

Related Commands[show ipv6 default-gateway \(643\)](#)[ip default-gateway \(624\)](#)

ipv6 address This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

Syntax

[no] ipv6 address *ipv6-address[/prefix-length]*

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command, or it can be automatically configured using the [ipv6 address autoconfig](#) command.
- ◆ If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- ◆ If a duplicate address is detected, a warning message is sent to the console.

Example

This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
```

```
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::1:ff00:72
    ff02::1:ff83:3466
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address eui-64 \(638\)](#)

[ipv6 address autoconfig \(636\)](#)

[show ipv6 interface \(643\)](#)

[ip address \(622\)](#)

ipv6 address autoconfig This command enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages; the host portion is based on the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address). Use the **no** form to remove the address generated by this command.

Syntax

[no] ipv6 address autoconfig

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address (if a global prefix is included in received router advertisements) and a link local address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- ◆ If a duplicate address is detected, a warning message is sent to the console.

- ◆ When DHCPv6 is restarted, the switch may attempt to acquire an IP address prefix through stateful address autoconfiguration. If the router advertisements have the “other stateful configuration” flag set, the switch may also attempt to acquire other non-address configuration information (such as a default gateway) from a DHCPv6 server when DHCPv6 is restarted.

Example

This example assigns a dynamic global unicast address of to the switch.

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale
Link-local address:
    fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
    2001:db8:2222:7272:7272:cfff:fe83:3466/64, subnet is 2001:db8:2222:7272::/
    64
    valid lifetime 2591531 preferred lifetime 604331
Joined group address(es):
    ff02::1:ff83:3466
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address \(635\)](#)

[show ipv6 interface \(643\)](#)

ipv6 address eui-64 This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

Syntax

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix/prefix-length* **eui-64**]

ipv6-prefix - The IPv6 network portion of the address assigned to the interface.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- ◆ Note that the value specified in the *ipv6-prefix* may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.
- ◆ If a duplicate address is detected, a warning message is sent to the console.
- ◆ IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.
- ◆ For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for

globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- ◆ This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

Example

This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
    2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64[EUI]
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::1:ff00:72
    ff02::1:ff83:3466
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address autoconfig \(636\)](#)

[show ipv6 interface \(643\)](#)

ipv6 address link-local This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

Syntax

ipv6 address *ipv6-address* link-local

no ipv6 address [*ipv6-address* link-local]

ipv6-address - The IPv6 address assigned to the interface.

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The specified address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be in the range of FE80~FEBF.
- ◆ The address specified with this command replaces a link-local address that was automatically generated for the interface.
- ◆ You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- ◆ If a duplicate address is detected, a warning message is sent to the console.

Example

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that a prefix in the range of FE80~FEBF is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
  2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64[EUI]
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
  ff02::1:ff19:6779
  ff02::1:ff00:72
  ff02::1:ff83:3466
```



```
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 enable \(641\)](#)

[show ipv6 interface \(643\)](#)

ipv6 enable This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

Syntax

[no] ipv6 enable

Default Setting

IPv6 is disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the switch's MAC address to modified EUI-64 format (see [page 638](#)). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.
- ◆ If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.
- ◆ The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

Example

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
```

```
IPv6 is enabled
Link-local address:
  fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
  2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64 [EUI]
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
  ff02::1:ff19:6779
  ff02::1:ff00:72
  ff02::1:ff83:3466
  ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address link-local \(640\)](#)

[show ipv6 interface \(643\)](#)

ipv6 mtu This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 mtu *size*

no ipv6 mtu

size - Specifies the MTU size. (Range: 1280-65535 bytes)

Default Setting

1500 bytes

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
- ◆ IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- ◆ All devices on the same physical medium must use the same MTU in order to operate correctly.
- ◆ IPv6 must be enabled on an interface before the MTU can be set.

Example

The following example sets the MTU for VLAN 1 to 1280 bytes:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

Related Commands

[show ipv6 mtu \(645\)](#)

[jumbo frame \(99\)](#)

show ipv6 default-gateway This command displays the current IPv6 default gateway.

Command Mode

Normal Exec, Privileged Exec

Example

The following shows the default gateway configured for this device:

```
Console#show ipv6 default-gateway
IPv6 default gateway 2001:DB8:2222:7272::254

Console#
```

show ipv6 interface This command displays the usability and configured settings for IPv6 interfaces.

Syntax

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix/prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

vlan-id - VLAN ID (Range: 1-4093)

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Command Mode

Privileged Exec

Example

This example displays all the IPv6 addresses configured for the switch.

```

Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
    2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64 [EUI]
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::1:ff19:6779
    ff02::1:ff00:72
    ff02::1:ff83:3466
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#

```

Table 135: show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked “up” if the switch can send and receive packets on this interface, “down” if a line signal is not present, or “administratively down” if the interface has been disabled by the administrator.
IPv6	IPv6 is marked “enable” if the switch can send and receive IP traffic on this interface, “disable” if the switch cannot send and receive IP traffic on this interface, or “stalled” if a duplicate link-local address is detected on the interface.
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface
Joined group address(es)	<p>In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively.</p> <p>FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.</p> <p>A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.</p>
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.

Table 135: show ipv6 interface - display description (Continued)

Field	Description
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.
ND retransmit interval	The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection.
ND advertised retransmit interval	The retransmit interval is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND reachable time	The amount of time a remote IPv6 node is considered reachable after a reachability confirmation event has occurred
ND advertised reachable time	The reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND advertised router lifetime	The length of time during which the prefix is valid for on-link determination.

This example displays a brief summary of IPv6 addresses configured on the switch.

```

Console#show ipv6 interface brief
Interface      VLAN      IPv6      IPv6 Address
-----
VLAN 1         Up        Up        2001:DB8:2222:7273::72/96
VLAN 1         Up        Up        FE80::2E0:CFE:FE00:FD%1/64
Console#

```

Related Commands

[show ip interface \(625\)](#)

show ipv6 mtu This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows the MTU cache for this device:

```

Console#show ipv6 mtu
MTU      Since      Destination Address
1400     00:04:21   5000:1::3
1280     00:04:50   FE80::203:A0FF:FED6:141D
Console#

```

Table 136: show ipv6 mtu - display description*

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

* No information is displayed if an IPv6 address has not been assigned to the switch.

show ipv6 traffic This command displays statistics about IPv6 traffic passing through this switch.

Command Mode

Privileged Exec

Example

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
    3 total received
    header errors
    too big errors
    no routes
    address errors
    unknown protocols
    truncated packets
    discards
    delivers
    reassembly request datagrams
    reassembly succeeded
    reassembly failed
IPv6 sent
    forwards datagrams
    6 requests
    discards
    no routes
    generated fragments
    fragment succeeded
    fragment failed
ICMPv6 Statistics:
ICMPv6 received
    input
    errors
    destination unreachable messages
    packet too big messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    router solicit messages
    router advertisement messages
    neighbor solicit messages
```

```

neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages

ICMPv6 sent
6 output
  destination unreachable messages
  packet too big messages
  time exceeded messages
  parameter problem message
  echo request messages
  echo reply messages
3 router solicit messages
  router advertisement messages
3 neighbor solicit messages
  neighbor advertisement messages
  redirect messages
  group membership query messages
  group membership response messages
  group membership reduction messages

UDP Statistics:
  input
  no port errors
  other errors
  output

Console#

```

Table 137: show ipv6 traffic - display description

Field	Description
<i>IPv6 Statistics</i>	
<i>IPv6 received</i>	
total received	The total number of input datagrams received by the interface, including those received in error.
header errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
too big errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
address errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
truncated packets	The number of input datagrams discarded because datagram frame didn't carry enough data.

Table 137: show ipv6 traffic - display description (Continued)

Field	Description
discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
reassembly request datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
reassembly succeeded	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
reassembly failed	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
<i>IPv6 sent</i>	
forwards datagrams	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.
requests	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> .
discards	The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> if any such packets met this (discretionary) discard criterion.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
generated fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
fragment succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
fragment failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.

Table 137: show ipv6 traffic - display description (Continued)

Field	Description
<i>ICMPv6 Statistics</i>	
<i>ICMPv6 received</i>	
input	The total number of ICMP messages received by the interface which includes all those counted by <code>ipv6IfIcmpInErrors</code> . Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
destination unreachable messages	The number of ICMP Destination Unreachable messages received by the interface.
packet too big messages	The number of ICMP Packet Too Big messages received by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages received by the interface.
parameter problem message	The number of ICMP Parameter Problem messages received by the interface.
echo request messages	The number of ICMP Echo (request) messages received by the interface.
echo reply messages	The number of ICMP Echo Reply messages received by the interface.
router solicit messages	The number of ICMP Router Solicit messages received by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages received by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages received by the interface.
neighbor advertisement messages	The number of ICMP Neighbor Advertisement messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
group membership query messages	The number of ICMPv6 Group Membership Query messages received by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages received by the interface.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
multicast listener discovery version 2 reports	The number of MLDv2 reports received by the interface.
<i>ICMPv6 sent</i>	
output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by <code>icmpOutErrors</code> .
destination unreachable messages	The number of ICMP Destination Unreachable messages sent by the interface.
packet too big messages	The number of ICMP Packet Too Big messages sent by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages sent by the interface.
parameter problem message	The number of ICMP Parameter Problem messages sent by the interface.

Table 137: show ipv6 traffic - display description (Continued)

Field	Description
echo request messages	The number of ICMP Echo (request) messages sent by the interface.
echo reply messages	The number of ICMP Echo Reply messages sent by the interface.
router solicit messages	The number of ICMP Router Solicitation messages sent by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages sent by the interface.
neighbor advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
redirect messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
group membership query messages	The number of ICMPv6 Group Membership Query messages sent by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages sent.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages sent.
multicast listener discovery version 2 reports	The number of MLDv2 reports sent by the interface.
<i>UDP Statistics</i>	
input	The total number of UDP datagrams delivered to UDP users.
no port errors	The total number of received UDP datagrams for which there was no application at the destination port.
other errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
output	The total number of UDP datagrams sent from this entity.

clear ipv6 traffic This command resets IPv6 traffic counters.

Command Mode
Privileged Exec

Command Usage

This command resets all of the counters displayed by the [show ipv6 traffic](#) command.

Example

```
Console#clear ipv6 traffic
Console#
```

ping6 This command sends (IPv6) ICMP echo request packets to another node on the network.

Syntax

ping6 {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 0-1500 bytes)

The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

count: 5

size: 32 bytes

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ When pinging a host name, be sure the DNS server has been enabled (see [page 599](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 600](#)).
- ◆ When using ping6 with a host name, the switch first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

Example

```
Console#ping6 FE80::2E0:CFF:FE00:FC%1
Press ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,
  timeout is 3 seconds
response time: 20 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 2
```

```
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 3
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
Console#
```

traceroute6 This command shows the route packets take to the specified destination.

Syntax

traceroute6 {*ipv6-address* | *host-name*} [**max-failures** *failure-count*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

failure-count - The maximum number of failures before which the trace route is terminated. (Range: 1-255)

Default Setting

Maximum failures: 5

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **traceroute6** command to determine the path taken to reach a specified destination.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function

prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

Example

```

Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1
Press "ESC" to abort.

Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3
seconds, 5 max failure(s) before termination.

Hop  Packet 1 Packet 2 Packet 3 IPv6 Address
-----
 1    <10 ms   <10 ms   <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.
Console#

```

Neighbor Discovery

ipv6 nd dad attempts This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

Syntax

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

Default Setting

3

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Configuring a value of 0 disables duplicate address detection.
- ◆ Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- ◆ Duplicate address detection is stopped on any interface that has been suspended (see the [vlan](#) command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.

- ◆ An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- ◆ If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
- ◆ If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

Example

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The `show ipv6 interface` command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::200:e8ff:fe90:0/64
Global unicast address(es):
    2009:db9:2229::79, subnet is 2009:db9:2229:0::/64
Joined group address(es):
    ff01::1/16
    ff02::1/16
    ff02::1:ff00:79/104
    ff02::1:ff90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

Related Commands

[ipv6 nd ns-interval \(655\)](#)
[show ipv6 neighbors \(657\)](#)

ipv6 nd ns-interval This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

Syntax

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

Default Setting

1000 milliseconds is used for neighbor discovery operations

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

Example

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::200:e8ff:FE90:0/64
Global unicast address(es):
    2009:db9:2229::79, subnet is 2009:db9:2229:0::/64
Joined group address(es):
    ff01::1/16
    ff02::1/16
    ff02::1:ff00:79/104
    ff02::1:ff90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

Related Commands

[show running-config \(93\)](#)

ipv6 nd reachable-time This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. Use the **no** form to restore the default setting.

Syntax

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability. (Range: 0-3600000)

Default Setting

30000 milliseconds is used for neighbor discovery operations
Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The time limit configured by this parameter allows the router to detect unavailable neighbors. During the neighbor discover process, an IPv6 node will multicast neighbor solicitation messages to search for neighbor nodes. For a neighbor node to be considered reachable, it must respond to the neighbor soliciting node with a neighbor advertisement message to become a confirmed neighbor, after which the reachable timer will be considered in effect for subsequent unicast IPv6 layer communications.

Example

The following sets the reachable time for a remote node to 1000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd reachable-time 1000
Console(config)#
```

clear ipv6 neighbors This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

Command Mode

Privileged Exec

Example

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```


show ipv6 neighbors This command displays information in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

vlan-id - VLAN ID (Range: 1-4094)

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

All IPv6 neighbor discovery cache entries are displayed.

Command Mode

Privileged Exec

Example

The following shows all known IPv6 neighbors for this switch:

```

Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                               Age  Link-layer Addr  State Interface
-----
FE80::2E0:CFF:FE9C:CA10                    4    00-E0-0C-9C-CA-10 R        1
Console#

```

Table 138: show ipv6 neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Addr	Physical layer MAC address.
State	<p>The following states are used for dynamic entries:</p> <p>I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.</p> <p>I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293).</p> <p>R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.</p> <p>S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.</p>

Table 138: show ipv6 neighbors - display description (Continued)

Field	Description
	<p>D (Delay) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.</p> <p>P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.</p> <p>U (Unknown) - Unknown state.</p> <p>The following states are used for static entries:</p> <p>I1 (Incomplete)-The interface for this entry is down.</p> <p>R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.</p> <p>P2 (Permanent) - Indicates a static entry.</p>
VLAN	VLAN interface from which the address was reached.

Related Commands

[show mac-address-table \(428\)](#)

IP Routing Commands

After network interfaces are configured for the switch, the paths used to send traffic between different interfaces must be set. To forward traffic to devices on other subnetworks, configure fixed paths with static routing commands. This section includes commands for static routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Table 160: IP Routing Commands

Command Group	Function
Global Routing Configuration	Configures global parameters for static routing, displays the routing table
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP

Global Routing Configuration

Table 161: Global Routing Configuration Commands

Command	Function	Mode
<i>IPv4 Commands</i>		
ip route	Configures static routes	GC
show ip route	Displays entries in the routing table	PE

IPv4 Commands

ip route This command configures static routes. Use the **no** form to remove static routes.

Syntax

ip route *destination-ip netmask next-hop [distance]*

no ip route {*destination-ip netmask next-hop* | *}

destination-ip – IP address of the destination network, subnetwork, or host.

netmask – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

next-hop – IP address of the next hop router used for this route.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distance used by the dynamic unicast routing protocol is 120 for RIP. (Range: 1-255, Default: 1)

* – Removes all static routing table entries.

Default Setting

No static routes are configured.

Command Mode

Global Configuration

Command Usage

- ◆ Up to 32 static routes can be configured.
- ◆ If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.

Example

This example forwards all traffic for subnet 192.168.1.0 to the gateway router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

show ip route This command displays information in the Forwarding Information Base (FIB).

Syntax

show ip route [**connected** | **database** | **rip** | **static** | **summary**]

connected – Displays all currently connected entries.

database – All known routes, including inactive routes.

rip – Displays all entries learned through the Routing Information Protocol (RIP).

static – Displays all static entries.

summary – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

Command Mode

Privileged Exec

Command Usage

- ◆ The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- ◆ This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any static route entry must be up.

Example

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       192.168.1.0/24 is directly connected, VLAN1
Console#
```

The RIB contains all available routes learned through directly attached networks, and any additionally configured routes such as static routes. The RIB contains the set of all available routes from which optimal entries are selected for use by the Forwarding Information Base (see Command Usage under the [show ip route](#) command).

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C    *> 192.168.1.0/24 is directly connected, VLAN1

Console#
```

In the following example, the numeric identifier following the routing table name (0) indicates the Forwarding Information Base identifier.

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 1
Connected          2
Total              2
Console#
```

Routing Information Protocol (RIP)

Table 162: Routing Information Protocol Commands

Command	Function	Mode
router rip	Enables the RIP routing protocol	GC
default-information originate	Generates a default external route into an autonomous system	RC
default-metric	Sets the default metric assigned to external routes imported from other protocols	RC
distance	Defines an administrative distance for external routes learned from other routing protocols	RC
maximum-prefix	Sets the maximum number of RIP routes allowed	RC
neighbor	Defines a neighboring router with which to exchange information	RC
network	Specifies the network interfaces that are to use RIP routing	RC
passive-interface	Stops RIP from sending routing updates on the specified interface	RC
redistribute	Redistribute routes from one routing domain to another	RC

Table 162: Routing Information Protocol Commands (Continued)

Command	Function	Mode
<code>timers basic</code>	Sets basic timers, including update, timeout, garbage collection	RC
<code>version</code>	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC
<code>ip rip authentication mode</code>	Specifies the type of authentication used for RIP2 packets	IC
<code>ip rip authentication string</code>	Enables authentication for RIP2 packets and specifies keys	IC
<code>ip rip receive version</code>	Sets the RIP receive version to use on a network interface	IC
<code>ip rip receive-packet</code>	Configures the interface to receive of RIP packets	IC
<code>ip rip send version</code>	Sets the RIP send version to use on a network interface	IC
<code>ip rip send-packet</code>	Configures the interface to send RIP packets	IC
<code>ip rip split-horizon</code>	Enables split-horizon or poison-reverse loop prevention	IC
<code>clear ip rip route</code>	Clears specified data from the RIP routing table	PE
<code>clear ip rip statistics</code>	Clears the RIP statistics in the switch.	PE
<code>show ip protocols rip</code>	Displays RIP process parameters	PE
<code>show ip rip</code>	Displays information about RIP routes and configuration settings	PE

router rip This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

[no] router rip

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- ◆ RIP is used to specify how routers exchange routing table information.
- ◆ This command is also used to enter router configuration mode.

Example

```
Console(config)#router rip
Console(config-router)#
```

Related Commands

[network \(667\)](#)

default-information originate This command generates a default external route into the local RIP autonomous system. Use the **no** form to disable this feature.

Syntax

[no] default-information originate

Default Setting

Disabled

Command Mode

Router Configuration

Command Usage

This command sets a default route for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

Example

```
Console(config-router)#default-information originate
Console(config-router)#
```

Related Commands

[ip route \(660\)](#)
[redistribute \(669\)](#)

default-metric This command sets the default metric assigned to external routes imported from other protocols. Use the **no** form to restore the default value.

Syntax

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to external routes. (Range: 1-15)

Default Setting

1

Command Mode

Router Configuration

Command Usage

- ◆ This command does not override the metric value set by the [redistribute](#) command. When a metric value has not been configured by the [redistribute](#) command, the **default-metric** command sets the metric value to be used for all imported external routes.
- ◆ The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- ◆ It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

Example

This example sets the default metric to 5.

```
Console(config-router)#default-metric 5
Console(config-router)#
```

Related Commands

[redistribute \(669\)](#)

distance This command defines an administrative distance for external routes learned from other routing protocols. Use the **no** form to restore the default setting.

Syntax

[no] distance *distance network-address netmask*

distance - Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255)

network-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

Default Setting

None

Command Mode

Router Configuration

Command Usage

- ◆ Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.
- ◆ The administrative distance is applied to all routes learned for the specified network.

Example

```
Console(config-router)#distance 2 192.168.3.0 255.255.255.0  
Console(config-router)#
```

maximum-prefix This command sets the maximum number of RIP routes allowed by the system. Use the **no** form to restore the default setting.

Syntax

maximum-prefix *maximum-routes*

no maximum-prefix

maximum-routes - The maximum number of RIP routes which can be installed in the routing table. (Range: 1-24)

Default Setting

24

Command Mode

Router Configuration

Command Usage

All the learned RIP routes may not be copied to the hardware tables in ASIC for fast data forwarding because of hardware resource limitations.

Example

This example sets the maximum number of RIP routes to 20.

```
Console(config-router)#maximum-prefix 20  
Console(config-router)#
```

neighbor This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

Syntax

[no] neighbor *ip-address*

ip-address - IP address of a neighboring router.

Default Setting

No neighbors are defined.

Command Mode

Router Configuration

Command Usage

- ◆ This command can be used to configure a static neighbor (specifically for point-to-point links) with which this router will exchange routing information, rather than relying on broadcast or multicast messages generated by the RIP protocol.
- ◆ Use this command in conjunction with the [passive-interface](#) command to control the routing updates sent to specific neighbors.

Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

Related Commands

[passive-interface \(668\)](#)

network This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

Syntax

[no] network {*ip-address netmask* | **vlan** *vlan-id*}

ip-address – IP address of a network directly connected to this router.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

vlan-id - VLAN ID. (Range: 1-4094)

Default Setting

No networks are specified.

Command Mode

Router Configuration

Command Usage

- ◆ RIP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.
- ◆ Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address `nnn.xxx.xxx.xxx` is entered, the first field (`nnn`) determines the class:
 - 0 - 127 is class A, and only the first field in the network address is used.
 - 128 - 191 is class B, and the first two fields in the network address are used.
 - 192 - 223 is class C, and the first three fields in the network address are used.

Example

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0 255.252.0.0
Console(config-router)#
```

Related Commands

[router rip \(663\)](#)

passive-interface This command stops RIP from sending routing updates on the specified interface. Use the **no** form to disable this feature.

Syntax

[no] passive-interface vlan *vlan-id*
vlan-id - VLAN ID. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Router Configuration

Command Usage

- ◆ If this command is used to stop sending routing updates on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on that interface will continue to be received and processed.
- ◆ Use this command in conjunction with the [neighbor](#) command to control the routing updates sent to specific neighbors.

Example

```
Console(config-router)#passive-interface vlan 1  
Console(config-router)#
```

Related Commands

[neighbor \(667\)](#)

redistribute This command imports external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into the autonomous system. Use the **no** form to disable this feature.

Syntax

[no] redistribute {connected | static} [metric *metric-value*]

connected - Imports routes that are established automatically just by enabling IP on an interface.

static - Static routes will be imported into this routing domain.

metric-value - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

Default Setting

redistribution - none

metric-value - set by the [default-metric](#) command

Command Mode

Router Configuration

Command Usage

- ◆ When a metric value has not been configured by the **redistribute** command, the [default-metric](#) command sets the metric value to be used for all imported external routes.
- ◆ A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- ◆ It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

Example

This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

Related Commands

[default-metric \(664\)](#)

timers basic This command configures the RIP update timer, timeout timer, and garbage-collection timer. Use the **no** form to restore the defaults.

Syntax

timers basic *update timeout garbage*

no timers basic

update – Sets the update timer to the specified value.
(Range: 5-2147483647 seconds)

timeout – Sets the timeout timer to the specified value. (Range: 90-360 seconds)

garbage – Sets the garbage collection timer to the specified value.
(Range: 60-240 seconds)

Default Setting

Update: 30 seconds

Timeout: 180 seconds

Garbage collection: 120 seconds

Command Mode

Router Configuration

Command Usage

- ◆ The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- ◆ The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- ◆ After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to it being purged by this device.

- ◆ Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- ◆ These timers must be set to the same values for all routers in the network.

Example

This example sets the: update timer to 40 seconds, the timeout timer to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 40 240 160
Console(config-router)#
```

version This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

Syntax

version {1 | 2}

no version

1 - RIP Version 1

2 - RIP Version 2

Default Setting

Receive: Accepts RIPv1 or RIPv2 packets

Send: Route information is broadcast to other routers with RIPv2.

Command Mode

Router Configuration

Command Usage

- ◆ When this command is used to specify a global RIP version, any VLAN interface not previously set by the [ip rip receive version](#) or [ip rip send version](#) command will use the global RIP version setting.
- ◆ When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the [ip rip receive version](#) or [ip rip send version](#) command will be set to the default send or receive version.
- ◆ Any configured interface settings take precedence over the global settings.

Example

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

Related Commands

[ip rip receive version \(673\)](#)

[ip rip send version \(675\)](#)

ip rip authentication mode This command specifies the type of authentication that can be used for RIPv2 packets. Use the **no** form to restore the default value.

Syntax

ip rip authentication mode {md5 | text}

no ip rip authentication mode

md5 - Message Digest 5 (MD5) authentication

text - Indicates that a simple password will be used.

Default Setting

Text authentication

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The password to be used for authentication is specified in the [ip rip authentication string](#) command.
- ◆ This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- ◆ For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.
- ◆ MD5 is a one-way hash algorithm that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

Related Commands

[ip rip authentication string \(673\)](#)

ip rip authentication string This command specifies an authentication key for RIPv2 packets. Use the **no** form to delete the authentication key.

Syntax

ip rip authentication string *key-string*

no ip rip authentication string

key-string - A password used for authentication.
(Range: 1-16 characters, case sensitive)

Default Setting

No authentication key

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- ◆ For authentication to function properly, both the sending and receiving interface must be configured with the same password, and authentication enabled by the [ip rip authentication mode](#) command.

Example

This example sets an authentication password of "small" to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication string small
Console(config-if)#
```

Related Commands

[ip rip authentication mode \(672\)](#)

ip rip receive version This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

Syntax

ip rip receive version {1 | 2}

no ip rip receive version

1 - Accepts only RIPv1 packets.

2 - Accepts only RIPv2 packets.

Default Setting

RIPv1 and RIPv2 packets

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Use this command to override the global setting specified by the RIP [version](#) command.
- ◆ You can specify the receive version based on these options:
 - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use the default of version 1 or 2 if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

Example

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

Related Commands

[version \(671\)](#)

ip rip receive-packet This command configures the interface to receive RIP packets. Use the **no** form to disable this feature.

Syntax

[no] ip rip receive-packet

Default Setting

Enabled

Command Mode

Interface Configuration (VLAN)

Default Setting

Enabled

Command Usage

Use the **no** form of this command if it is not required to add any dynamic entries to the routing table for an interface. For example, when only static routes are to be allowed for a specific interface.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive-packet
Console(config-if)#
```

Related Commands

[ip rip send-packet \(676\)](#)

ip rip send version This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

Syntax

ip rip send version {1 | 2 | 1-compatible}

no ip rip send version

1 - Sends only RIPv1 packets.

2 - Sends only RIPv2 packets.

1-compatible - Route information is broadcast to other routers with RIPv2.

Default Setting

1-compatible (Route information is broadcast to other routers with RIPv2)

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Use this command to override the global setting specified by the RIP [version](#) command.
- ◆ You can specify the send version based on these options:
 - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use "1-compatible" to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information.)

Example

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

Related Commands

[version \(671\)](#)

ip rip send-packet This command configures the interface to send RIP packets. Use the **no** form to disable this feature.

[no] ip rip send-packet

Default Setting

Enabled

Command Mode

Interface Configuration (VLAN)

Default Setting

Enabled

Command Usage

The **no** form of this command allows the router to passively monitor route information advertised by other routers attached to the network, without transmitting any RIP updates.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send-packet
Console(config-if)#
```

Related Commands

[ip rip receive-packet \(674\)](#)

ip rip split-horizon This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable this function.

Syntax

ip rip split-horizon [poisoned]

no ip ip split-horizon

poisoned - Enables poison-reverse on the current interface.

Command Mode

Interface Configuration (VLAN)

Default Setting

split-horizon poisoned

Command Usage

- ◆ Split horizon never propagates routes back to an interface from which they have been acquired.
- ◆ Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)
- ◆ If split-horizon is disabled with the **no rip ip split-horizon** command, and a loop occurs, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

clear ip rip route This command clears specified data from the RIP routing table.

Syntax

clear ip rip route {*ip-address netmask* | **all** | **connected** | **rip** | **static**}

ip-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

all - Deletes all entries from the routing table.

connected - Deletes all currently connected entries.

rip - Deletes all entries learned through the Routing Information Protocol.

static - Deletes all static entries.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command with the “all” parameter clears the RIP table of all routes. To avoid deleting the entire RIP network, use the [redistribute connected](#) command to make the RIP network a connected route. To delete the RIP routes learned from neighbors and also keep the RIP network intact, use the “rip” parameter with this command (**clear ip rip route rip**).

Example

This example clears one specific route.

```
Console#clear ip rip route 192.168.1.0 255.255.255.0
Console#
```

clear ip rip statistics This command clears the RIP routing counters.

Syntax

clear ip rip statistics

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Issuing this command from the Privileged Exec. level will clear all RIP statistics collected by the switch.

Example

This example clears the RIP statistics.

```
Console#clear ip rip statistics
Console#
```

show ip protocols rip This command displays RIP process parameters.

Command Mode

Privileged Exec

Example

```

Console#show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 40 seconds with +/-5 seconds
  Timeout after 240 seconds, garbage collect after 160 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version by interface set, receive version by
  inte
rface set
    Interface  Send          Recv  Bad Packets  Bad Routes  Send Updates
    VLAN1      1-compatible  1 2    0             0             0
Routing for Networks:
  10.0.0.0/14
Routing Information Sources:
  Gateway      Distance  Last Update  Version  Bad Packets  Bad Routes
The maximum number of RIP routes allowed: 20
Distance: Default is 120
Console#

```

show ip rip This command displays information about RIP routes and configuration settings. Use this command without any keywords to display all RIP routes.

Syntax

show ip rip [**interface** [**vlan** *vlan-id*]]

interface - Shows RIP configuration settings for all interfaces or for a specified interface.

vlan-id - VLAN ID. (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       C - Connected, S - Static, O - OSPF

      Network            Next Hop          Metric From      Interface Time
Rc 192.168.0.0/24                1              VLAN1      01:57
Console#show ip rip interface vlan 1
Interface: vlan1
Routing Protocol: RIP
  Receive RIPv1 and RIPv2 packets
  Send RIPv1 Compatible
  Passive interface: Disabled
  Authentication mode: (None)
  Authentication string: (None)
  Split horizon: Enabled with Poisoned Reverse
  IP interface address: 192.168.0.2/24
Console#
```


Section III

Appendices

This section provides additional information and includes these items:

- ◆ [“Troubleshooting” on page 683](#)
- ◆ [“License Information” on page 685](#)



Troubleshooting

Problems Accessing the Management Interface

Table 163: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, or SNMP software	<ul style="list-style-type: none">◆ Be sure the switch is powered up.◆ Check network cabling between the management station and the switch. Make sure the ends are properly connected and there is no damage to the cable. Test the cable if necessary.◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled.◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway.◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	<ul style="list-style-type: none">◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station.◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service. Try using another SSH client or check for updates to your SSH client application.◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none">◆ Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 115200 bps.◆ Verify that you are using the RJ-45 to DB-9 null-modem serial cable supplied with the switch. If you use any other cable, be sure that it conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	<ul style="list-style-type: none">◆ Contact your local distributor.

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the “show tech-support” command to record all system settings in this file.
9. Contact your distributor’s service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
:
```



License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
- 7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP Option 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DHCP Snooping A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

- DiffServ** Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.
- DNS** Domain Name Service. A system used for translating host names for network nodes into IP addresses.
- DSCP** Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.
- EAPOL** Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.
- EUI** Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.
- GARP** Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.
- GMRP** Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.
- ICMP** Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

- IEEE 802.1D** Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.
- IEEE 802.1Q** VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.
- IEEE 802.1p** An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.
- IEEE 802.1s** An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.
- IEEE 802.1w** An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)
- IEEE 802.1X** Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.
- IEEE 802.3ac** Defines frame extensions for VLAN tagging.
- IEEE 802.3x** Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)
- IGMP** Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.
- IGMP Proxy** Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in a simple tree that uses IGMP Proxy.
- IGMP Query** On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP Snooping Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

In-Band Management Management of the network from a station attached directly to the network.

IP Multicast Filtering A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Layer 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MRD Multicast Router Discovery is a protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

MSTP Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

Multicast Switching A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management Management of the network from a station not attached to the network.

Port Authentication See *IEEE 802.1X*.

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

QinQ QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QoS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP Routing Information Protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SMTP Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Telnet Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

List of CLI Commands

aaa accounting commands 216
aaa accounting dot1x 217
aaa accounting exec 218
aaa accounting update 219
aaa authorization commands 219
aaa authorization exec 220
aaa group server 221
absolute 150
access-list arp 344
access-list ip 326
access-list ipv6 332
access-list mac 339
accounting commands 223
accounting dot1x 222
accounting exec 223
arp 630
authentication enable 204
authentication login 205
authorization commands 224
authorization exec 225
boot system 102
calendar set 148
capabilities 351
channel-group 382
class 506
class-map 502
clear access-list hardware counters 347
clear arp-cache 632
clear counters 357
clear dns cache 603
clear host 603
clear ip dhcp snooping binding 295
clear ip dhcp snooping database flash 295
clear ip igmp snooping groups dynamic 530
clear ip igmp snooping statistics 530
clear ip rip route 677
clear ip rip statistics 678
clear ip source-guard binding blocked 303
clear ipv6 mld snooping groups dynamic 555
clear ipv6 mld snooping statistics 555
clear ipv6 neighbors 656
clear ipv6 traffic 650
clear log 129
clear mac-address-table dynamic 427
clear network-access 274
clock summer-time (date) 143
clock summer-time (predefined) 145
clock summer-time (recurring) 146
clock timezone 147
cluster 153
cluster commander 154
cluster ip-pool 155
cluster member 156
configure 83
copy 103
databits 115
default-information originate 664
default-metric 664
delete 107
delete public-key 239
description 503
description 352
dir 108
disable 84
disconnect 122
distance 665
dos-protection echo-charge 314
dos-protection smurf 315
dos-protection tcp-flooding 315
dos-protection tcp-null-scan 316
dos-protection tcp-syn-fin-scan 316
dos-protection tcp-xmas-scan 317
dos-protection udp-flooding 317
dos-protection win-nuke 318
dot1q-tunnel system-tunnel-control 472
dot1q-tunnel tpid 473
dot1x default 244
dot1x intrusion-action 246
dot1x max-reauth-req 246
dot1x max-req 247
dot1x operation-mode 248
dot1x port-control 249
dot1x re-authenticate 252
dot1x re-authentication 249
dot1x system-auth-control 245
dot1x timeout quiet-period 250
dot1x timeout re-authperiod 250
dot1x timeout supp-timeout 251
dot1x timeout tx-period 251
enable 81
enable password 200
end 85

List of CLI Commands

exec-timeout 116
exit 85
flowcontrol 353
history 354
hostname 88
interface 350
interface vlan 464
ip access-group 330
ip address 622
ip arp inspection 306
ip arp inspection filter 307
ip arp inspection limit 311
ip arp inspection log-buffer logs 308
ip arp inspection trust 311
ip arp inspection validate 309
ip arp inspection vlan 310
ip default-gateway 624
ip dhcp client class-id 609
ip dhcp dynamic-provision 608
ip dhcp relay server 615
ip dhcp restart client 611
ip dhcp restart relay 616
ip dhcp snooping 283
ip dhcp snooping max-number 294
ip dhcp snooping database flash 296
ip dhcp snooping information option 285
ip dhcp snooping information option circuit-id 292
ip dhcp snooping information option encode no-subtype 286
ip dhcp snooping information option remote-id 288
ip dhcp snooping information option tr101 board-id 289
ip dhcp snooping information policy 289
ip dhcp snooping trust 294
ip dhcp snooping verify mac-address 290
ip dhcp snooping vlan 291
ip domain-list 598
ip domain-lookup 599
ip domain-name 600
ip host 600
ip http authentication 228
ip http port 228
ip http secure-port 229
ip http secure-server 230
ip http server 229
ip igmp filter (Global Configuration) 538
ip igmp filter (Interface Configuration) 540
ip igmp max-groups 541
ip igmp max-groups action 541
ip igmp profile 538
ip igmp query-drop 542
ip igmp snooping 515
ip igmp snooping proxy-reporting 516
ip igmp snooping querier 516
ip igmp snooping router-alert-option-check 517
ip igmp snooping router-port-expire-time 517
ip igmp snooping tcn-flood 518
ip igmp snooping tcn-query-solicit 519
ip igmp snooping unregistered-data-flood 520
ip igmp snooping unsolicited-report-interval 520
ip igmp snooping version 521
ip igmp snooping version-exclusive 522
ip igmp snooping vlan general-query-suppression 522
ip igmp snooping vlan immediate-leave 523
ip igmp snooping vlan last-memb-query-count 524
ip igmp snooping vlan last-memb-query-intvl 525
ip igmp snooping vlan mrd 525
ip igmp snooping vlan mrouter 536
ip igmp snooping vlan proxy-address 526
ip igmp snooping vlan query-interval 528
ip igmp snooping vlan query-resp-intvl 528
ip igmp snooping vlan static 529
ip mdns 605
ip multicast-data-drop 628
ip name-server 601
ip proxy-arp 631
ip rip authentication mode 672
ip rip authentication string 673
ip rip receive version 673
ip rip receive-packet 674
ip rip send version 675
ip rip send-packet 676
ip rip split-horizon 676
ip route 660
ip source-guard 300
ip source-guard binding 298
ip source-guard max-binding 301
ip source-guard mode 302
ip ssh authentication-retries 237
ip ssh crypto host-key generate 240
ip ssh crypto zeroize 241
ip ssh save host-key 241
ip ssh server 237
ip ssh server-key size 238
ip ssh timeout 239
ip telnet max-sessions 232
ip telnet port 232
ip telnet server 233
ip tftp retry 112
ip tftp timeout 113
ipv6 access-group 337
ipv6 address 635
ipv6 address autoconfig 636
ipv6 address eui-64 638
ipv6 address link-local 640
ipv6 default-gateway 634
ipv6 dhcp client rapid-commit vlan 612
ipv6 dhcp relay destination 617
ipv6 dhcp relay destination multicast 618

ipv6 dhcp restart client vlan 612
 ipv6 enable 641
 ipv6 host 602
 ipv6 mld filter (Global Configuration) 564
 ipv6 mld filter (Interface Configuration) 567
 ipv6 mld max-groups 567
 ipv6 mld max-groups action 568
 ipv6 mld profile 565
 ipv6 mld query-drop 569
 ipv6 mld snooping 547
 ipv6 mld snooping proxy-reporting 547
 ipv6 mld snooping querier 548
 ipv6 mld snooping query-interval 549
 ipv6 mld snooping query-max-response-time 549
 ipv6 mld snooping robustness 550
 ipv6 mld snooping router-port-expire-time 550
 ipv6 mld snooping unknown-multicast mode 551
 ipv6 mld snooping unsolicited-report-interval 552
 ipv6 mld snooping version 552
 ipv6 mld snooping vlan immediate-leave 553
 ipv6 mld snooping vlan mrouter 553
 ipv6 mld snooping vlan static 554
 ipv6 mtu 642
 ipv6 nd dad attempts 653
 ipv6 nd ns-interval 655
 ipv6 nd reachable-time 656
 jumbo frame 99
 lacp 383
 lacp admin-key (Ethernet Interface) 384
 lacp admin-key (Port Channel) 387
 lacp port-priority 385
 lacp system-priority 386
 lacp timeout 388
 line 115
 lldp 575
 lldp admin-status 579
 lldp basic-tlv management-ip-address 579
 lldp basic-tlv port-description 580
 lldp basic-tlv system-capabilities 580
 lldp basic-tlv system-description 581
 lldp basic-tlv system-name 581
 lldp dot1-tlv proto-ident 582
 lldp dot1-tlv proto-vid 582
 lldp dot1-tlv pvid 583
 lldp dot1-tlv vlan-name 583
 lldp dot3-tlv link-aggr 584
 lldp dot3-tlv mac-phy 584
 lldp dot3-tlv max-frame 585
 lldp dot3-tlv poe 585
 lldp holdtime-multiplier 575
 lldp med-fast-start-count 576
 lldp med-location civic-addr 586
 lldp med-notification 588
 lldp med-tlv ext-poe 588
 lldp med-tlv inventory 589
 lldp med-tlv location 589
 lldp med-tlv med-cap 590
 lldp med-tlv network-policy 590
 lldp notification 591
 lldp notification-interval 576
 lldp refresh-interval 577
 lldp reinit-delay 577
 lldp tx-delay 578
 logging command 125
 logging facility 126
 logging history 126
 logging host 127
 logging on 128
 logging sendmail 133
 logging sendmail destination-email 133
 logging sendmail host 134
 logging sendmail level 134
 logging sendmail source-email 135
 logging trap 129
 login 117
 loopback detection trap 422
 loopback-detection 420
 loopback-detection action 420
 loopback-detection recover-time 421
 loopback-detection release 423
 loopback-detection transmit-interval 422
 mac access-group 342
 mac-address-table aging-time 425
 mac-address-table static 426
 mac-authentication intrusion-action 273
 mac-authentication max-mac-count 273
 mac-authentication reauth-time 267
 mac-learning 260
 mac-vlan 480
 management 255
 match 504
 max-hops 440
 maximum-prefix 666
 media-type 354
 memory 180
 mst priority 441
 mst vlan 441
 name 442
 negotiation 355
 neighbor 667
 network 667
 network-access aging 265
 network-access dynamic-qos 268
 network-access dynamic-vlan 269
 network-access guest-vlan 270
 network-access mac-filter 266
 network-access max-mac-count 270
 network-access mode mac-authentication 271

List of CLI Commands

network-access port-mac-filter 272
nlm 177
no rspan session 410
ntp authenticate 140
ntp authentication-key 140
ntp client 141
ntp server 142
parity 118
passive-interface 668
password 118
password-thresh 119
periodic 151
permit, deny 539
permit, deny 565
permit, deny (ARP ACL) 345
permit, deny (Extended IPv4 ACL) 327
permit, deny (Extended IPv6 ACL) 334
permit, deny (MAC ACL) 340
permit, deny (Standard IP ACL) 326
permit, deny (Standard IPv6 ACL) 333
ping 627
ping6 651
police rate 507
policy-map 505
port channel load-balance 380
port monitor 403
port security 261
power inline 396
power inline compatible 393
power inline maximum allocation 396
power inline maximum allocation mode 394
power inline priority 397
power inline time-range 398
power mainpower maximum allocation 395
power-save 377
privilege 203
process cpu 181
process cpu guard 182
prompt 79
protocol-vlan protocol-group (Configuring Groups) 477
protocol-vlan protocol-group (Configuring Interfaces) 477
qos map cos-queue 494
qos map dscp-queue 496
qos map trust-mode 497
queue mode 490
queue weight 491
quit 82
radius-server acct-port 206
radius-server auth-port 207
radius-server encrypted-key 209
radius-server host 207
radius-server key 208
radius-server retransmit 209
radius-server timeout 210
range 539
range 566
rate-limit 414
rcommand 156
redistribute 669
reload (Global Configuration) 80
reload (Privileged Exec) 84
rename 505
revision 443
rmon alarm 186
rmon collection history 188
rmon collection rmon1 189
rmon event 187
router rip 663
rspan destination 408
rspan remote vlan 409
rspan source 407
server 222
service-policy 509
set cos 508
set ip dscp 509
sflow owner 193
sflow polling instance 195
sflow sampling instance 196
show access-group 347
show access-list 348
show access-list arp 346
show access-list tcam-utilization 89
show accounting 225
show arp 632
show authorization 226
show cable-diagnostics 376
show calendar 149
show class-map 510
show cluster 157
show cluster candidates 158
show cluster members 157
show dns 604
show dns cache 604
show dos-protection 318
show dot1q-tunnel 475
show dot1x 253
show history 82
show hosts 605
show interfaces brief 358
show interfaces counters 359
show interfaces history 363
show interfaces protocol-vlan protocol-group 479
show interfaces status 364
show interfaces switchport 365
show interfaces transceiver 373
show interfaces transceiver-threshold 374
show ip access-group 331
show ip access-list 331

show ip arp inspection configuration 312
show ip arp inspection interface 312
show ip arp inspection log 313
show ip arp inspection statistics 313
show ip arp inspection vlan 313
show ip dhcp dynamic-provision 611
show ip dhcp snooping 296
show ip dhcp snooping binding 297
show ip igmp filter 543
show ip igmp profile 543
show ip igmp query-drop 544
show ip igmp snooping 531
show ip igmp snooping group 532
show ip igmp snooping mrouter 533
show ip igmp snooping statistics 533
show ip igmp throttle interface 545
show ip interface 625
show ip mdns 606
show ip multicast-data-drop 629
show ip protocols rip 679
show ip rip 679
show ip route 661
show ip source-guard 303
show ip source-guard binding 304
show ip ssh 242
show ip telnet 234
show ip tftp 113
show ip traffic 625
show ipv6 access-group 337
show ipv6 access-list 338
show ipv6 default-gateway 643
show ipv6 dhcp duid 614
show ipv6 dhcp relay destination interface 619
show ipv6 dhcp vlan 614
show ipv6 interface 643
show ipv6 mld filter 569
show ipv6 mld profile 570
show ipv6 mld query-drop 570
show ipv6 mld snooping group 556
show ipv6 mld snooping mrouter 559
show ipv6 mld snooping statistics 559
show ipv6 mld throttle interface 572
show ipv6 mld snooping 556
show ipv6 mtu 645
show ipv6 neighbors 657
show ipv6 traffic 646
show lacp 389
show line 124
show lldp config 592
show lldp info local-device 593
show lldp info remote-device 594
show lldp info statistics 596
show log 130
show logging 131
show logging sendmail 135
show loopback-detection 423
show mac access-group 343
show mac access-list 343
show mac-address-table 428
show mac-address-table aging-time 429
show mac-address-table count 429
show mac-vlan 481
show management 256
show memory 90
show network-access 274
show network-access mac-address-table 275
show network-access mac-filter 276
show nlm oper-status 180
show ntp 143
show policy-map 511
show policy-map interface 511
show port monitor 404
show port security 263
show port-channel load-balance 392
show power inline status 399
show power inline time-range 400
show power mainpower 401
show power-save 378
show privilege 203
show process cpu 91
show process cpu guard 91
show process cpu task 92
show protocol-vlan protocol-group 478
show public-key 242
show qos map cos-queue 498
show qos map dscp-queue 499
show qos map trust-mode 499
show queue mode 493
show queue weight 493
show radius-server 210
show reload 85
show rmon alarms 190
show rmon events 190
show rmon history 191
show rmon statistics 191
show rspan 411
show running-config 93
show sflow 197
show snmp 163
show snmp engine-id 174
show snmp group 175
show snmp notify-filter 180
show snmp user 176
show snmp view 177
show snmp-server enable port-traps 168
show snmp 139
show spanning-tree 457
show spanning-tree mst configuration 460

List of CLI Commands

show ssh 243
show startup-config 95
show system 95
show tacacs-server 215
show tech-support 96
show time-range 152
show traffic-segmentation 323
show upgrade 112
show users 97
show version 98
show vlan 470
show voice vlan 488
show watchdog 99
show web-auth 281
show web-auth interface 281
show web-auth summary 282
shutdown 356
silent-time 120
snmp-server 161
snmp-server community 161
snmp-server contact 162
snmp-server enable port-traps link-up-down 167
snmp-server enable port-traps mac-notification 168
snmp-server enable traps 164
snmp-server engine-id 169
snmp-server group 170
snmp-server host 165
snmp-server location 162
snmp-server notify-filter 178
snmp-server user 171
snmp-server view 173
snmp client 137
snmp poll 138
snmp server 138
spanning-tree 432
spanning-tree bpdu-filter 443
spanning-tree bpdu-guard 444
spanning-tree cisco-prestandard 433
spanning-tree cost 445
spanning-tree edge-port 447
spanning-tree forward-time 433
spanning-tree hello-time 434
spanning-tree link-type 448
spanning-tree loopback-detection 448
spanning-tree loopback-detection action 449
spanning-tree loopback-detection release 456
spanning-tree loopback-detection release-mode 450
spanning-tree loopback-detection trap 451
spanning-tree max-age 435
spanning-tree mode 435
spanning-tree mst configuration 437
spanning-tree mst cost 451
spanning-tree mst port-priority 452
spanning-tree pathcost method 437
spanning-tree port-bpdu-flooding 453
spanning-tree port-priority 453
spanning-tree priority 438
spanning-tree protocol-migration 457
spanning-tree root-guard 454
spanning-tree spanning-disabled 455
spanning-tree system-bpdu-flooding 439
spanning-tree tc-prop-stop 455
spanning-tree transmission-limit 439
speed 121
speed-duplex 356
stopbits 121
switchport acceptable-frame-types 465
switchport allowed vlan 465
switchport dot1q-tunnel mode 474
switchport dot1q-tunnel priority map 474
switchport forbidden vlan 467
switchport ingress-filtering 467
switchport mode 468
switchport native vlan 469
switchport packet-rate 416
switchport priority default 492
switchport voice vlan 485
switchport voice vlan priority 486
switchport voice vlan rule 486
switchport voice vlan security 487
tacacs-server encrypted-key 213
tacacs-server host 211
tacacs-server key 212
tacacs-server port 213
tacacs-server retransmit 214
tacacs-server timeout 214
telnet (client) 233
terminal 123
test cable-diagnostics 375
timeout login response 122
time-range 149
timers basic 670
traceroute 626
traceroute6 652
traffic-segmentation 319
traffic-segmentation session 320
traffic-segmentation uplink/downlink 321
traffic-segmentation uplink-to-uplink 322
transceiver-monitor 367
transceiver-threshold current 368
transceiver-threshold rx-power 369
transceiver-threshold temperature 370
transceiver-threshold tx-power 371
transceiver-threshold voltage 372
transceiver-threshold-auto 368
upgrade opcode auto 109
upgrade opcode path 110
upgrade opcode reload 111

username 201
version 671
vlan 462
vlan database 462
voice vlan 482
voice vlan aging 483
voice vlan mac-address 484
watchdog software 99
web-auth 279
web-auth login-attempts 277
web-auth quiet-period 278
web-auth re-authenticate (IP) 280
web-auth re-authenticate (Port) 280
web-auth session-timeout 278
web-auth system-auth-control 279
whichboot 109

