



ECS4100 Series

ECS4100-26TX

ECS4100-26TX-ME

ECS4100-28T

ECS4100-52T

26/28/52-Port 10G/1G  
L2+ Ethernet Switches

Software Release  
v1.11.08.164

CLI Reference Guide

# CLI Reference Guide

---

## **ECS4100-26TX 10G Ethernet Switch**

26-Port L2+ 10G Ethernet Switch  
with 24 10/100/1000BASE-T (RJ-45) Ports  
and 2 10G SFP Ports

## **ECS4100-26TX-ME 10G Ethernet Switch**

26-Port L2+ 10G Ethernet Switch  
with 24 10/100/1000BASE-T (RJ-45) Ports  
2 10G SFP Ports  
and dual AC and DC power inputs

## **ECS4100-28T Gigabit Ethernet Switch**

28-Port L2+ Gigabit Ethernet Switch  
with 24 10/100/1000BASE-T (RJ-45) Ports  
and 4 Gigabit SFP Ports

## **ECS4100-52T Gigabit Ethernet Switch**

52-Port L2+ Gigabit Ethernet Switch  
with 48 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:

*Web Management Guide*

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.

<i>Revision</i>	<i>Date</i>	<i>Change Description</i>
V1.11.08.164	01/2017	Initial release

---

# Contents

<b>How to Use This Guide</b>	<b>3</b>
<b>Contents</b>	<b>5</b>
<b>Tables</b>	<b>35</b>

---

<b>Section I</b>	<b>Getting Started</b>	<b>41</b>
	<b>1 Initial Switch Configuration</b>	<b>43</b>
	Connecting to the Switch	43
	Configuration Options	43
	Connecting to the Console Port	44
	Logging Onto the Command Line Interface	45
	Setting Passwords	45
	Remote Connections	46
	Configuring the Switch for Remote Management	47
	Using the Network Interface	47
	Setting an IP Address	47
	Enabling SNMP Management Access	53
	Managing System Files	55
	Upgrading the Operation Code	56
	Saving or Restoring Configuration Settings	56
	Automatic Installation of Operation Code and Configuration Settings	58
	Downloading Operation Code from a File Server	58
	Specifying a DHCP Client Identifier	61
	Downloading a Configuration File and Other Parameters from a DHCP Server	62
	Setting the System Clock	64
	Setting the Time Manually	64
	Configuring SNTP	65
	Configuring NTP	65

<b>Section II</b>	<b>Command Line Interface</b>	<b>67</b>
<b>2</b>	<b>Using the Command Line Interface</b>	<b>69</b>
	Accessing the CLI	69
	Console Connection	69
	Telnet Connection	70
	Entering Commands	71
	Keywords and Arguments	71
	Minimum Abbreviation	71
	Command Completion	71
	Getting Help on Commands	72
	Partial Keyword Lookup	74
	Negating the Effect of Commands	74
	Using Command History	74
	Understanding Command Modes	74
	Exec Commands	75
	Configuration Commands	76
	Command Line Processing	77
	Showing Status Information	78
	CLI Command Groups	79
<b>3</b>	<b>General Commands</b>	<b>81</b>
	prompt	81
	reload (Global Configuration)	82
	enable	83
	quit	84
	show history	84
	configure	85
	disable	86
	reload (Privileged Exec)	86
	show reload	87
	end	87
	exit	87

<b>4 System Management Commands</b>	<b>89</b>
Device Designation	89
hostname	90
System Status	90
show access-list tcam-utilization	91
show memory	92
show process cpu	93
show process cpu guard	93
show process cpu task	94
show running-config	96
show startup-config	97
show system	98
show tech-support	99
show users	100
show version	101
show watchdog	101
watchdog software	102
Frame Size	102
jumbo frame	102
File Management	103
General Commands	104
boot system	104
copy	105
delete	109
dir	110
whichboot	111
Automatic Code Upgrade Commands	111
upgrade opcode auto	111
upgrade opcode path	113
upgrade opcode reload	114
show upgrade	114
TFTP Configuration Commands	114
ip tftp retry	114
ip tftp timeout	115
show ip tftp	115

Line	116
line	117
databits	118
exec-timeout	118
login	119
parity	120
password	121
password-thresh	121
silent-time	122
speed	123
stopbits	123
timeout login response	124
disconnect	125
terminal	125
show line	126
Event Logging	127
logging command	127
logging facility	128
logging history	128
logging host	129
logging on	130
logging trap	131
clear log	131
show log	132
show logging	133
SMTP Alerts	134
logging sendmail	135
logging sendmail destination-email	135
logging sendmail host	136
logging sendmail level	136
logging sendmail source-email	137
show logging sendmail	138
Time	138
SMTP Commands	139
sntp client	139



ntp poll	140
ntp server	140
show ntp	141
NTP Commands	142
ntp authenticate	142
ntp authentication-key	142
ntp client	143
ntp server	144
show ntp	145
Manual Configuration Commands	145
clock summer-time (date)	145
clock summer-time (predefined)	147
clock summer-time (recurring)	148
clock timezone	149
calendar set	150
show calendar	151
Time Range	151
time-range	151
absolute	152
periodic	153
show time-range	154
Switch Clustering	154
cluster	155
cluster commander	156
cluster ip-pool	157
cluster member	158
rcommand	158
show cluster	159
show cluster members	159
show cluster candidates	160
<b>5 SNMP Commands</b>	<b>161</b>
General SNMP Commands	163
snmp-server	163
snmp-server community	163

snmp-server contact	164
snmp-server location	165
show snmp	165
SNMP Target Host Commands	166
snmp-server enable traps	166
snmp-server host	167
snmp-server enable port-traps link-up-down	169
snmp-server enable port-traps mac-notification	170
show snmp-server enable port-traps	170
SNMPv3 Commands	171
snmp-server engine-id	171
snmp-server group	172
snmp-server user	173
snmp-server view	175
show snmp engine-id	176
show snmp group	177
show snmp user	178
show snmp view	179
Notification Log Commands	179
nlm	179
snmp-server notify-filter	180
show nlm oper-status	182
show snmp notify-filter	182
Additional Trap Commands	182
memory	182
process cpu	183
process cpu guard	184
<b>6 Remote Monitoring Commands</b>	<b>187</b>
rmon alarm	188
rmon event	189
rmon collection history	190
rmon collection rmon1	191
show rmon alarms	192
show rmon events	192

show rmon history	193
show rmon statistics	193
<b>7 Flow Sampling Commands</b>	<b>195</b>
sflow owner	195
sflow polling instance	197
sflow sampling instance	198
show sflow	199
<b>8 Authentication Commands</b>	<b>201</b>
User Accounts and Privilege Levels	202
enable password	202
username	203
privilege	205
show privilege	205
Authentication Sequence	206
authentication enable	206
authentication login	207
RADIUS Client	208
radius-server acct-port	208
radius-server auth-port	209
radius-server host	209
radius-server key	210
radius-server retransmit	211
radius-server timeout	211
show radius-server	212
TACACS+ Client	212
tacacs-server host	213
tacacs-server key	213
tacacs-server port	214
tacacs-server retransmit	214
tacacs-server timeout	215
show tacacs-server	215
AAA	216
aaa accounting commands	217
aaa accounting dot1x	218

aaa accounting exec	219
aaa accounting update	220
aaa authorization commands	220
aaa authorization exec	221
aaa group server	222
server	223
accounting dot1x	223
accounting commands	224
accounting exec	224
authorization commands	225
authorization exec	226
show accounting	226
show authorization	227
Web Server	228
ip http authentication	229
ip http port	229
ip http server	230
ip http secure-port	230
ip http secure-server	231
Telnet Server	232
ip telnet max-sessions	233
ip telnet port	233
ip telnet server	234
telnet (client)	234
show ip telnet	235
Secure Shell	235
ip ssh authentication-retries	238
ip ssh server	238
ip ssh server-key size	239
ip ssh timeout	240
delete public-key	240
ip ssh crypto host-key generate	241
ip ssh crypto zeroize	242
ip ssh save host-key	242
show ip ssh	243

show public-key	243
show ssh	244
802.1X Port Authentication	245
General Commands	246
dot1x default	246
dot1x system-auth-control	246
Authenticator Commands	247
dot1x intrusion-action	247
dot1x max-reauth-req	248
dot1x max-req	248
dot1x operation-mode	249
dot1x port-control	250
dot1x re-authentication	250
dot1x timeout quiet-period	251
dot1x timeout re-authperiod	251
dot1x timeout supp-timeout	252
dot1x timeout tx-period	252
dot1x re-authenticate	253
Supplicant Commands	254
dot1x timeout auth-period	254
dot1x timeout held-period	254
Information Display Commands	255
show dot1x	255
Management IP Filter	257
management	257
show management	258
PPPoE Intermediate Agent	259
pppoe intermediate-agent	260
pppoe intermediate-agent format-type	260
pppoe intermediate-agent port-enable	261
pppoe intermediate-agent port-format-type	262
pppoe intermediate-agent trust	263
pppoe intermediate-agent vendor-tag strip	264
clear pppoe intermediate-agent statistics	264
show pppoe intermediate-agent info	265

show pppoe intermediate-agent statistics	265
<b>9 General Security Measures</b>	<b>267</b>
Port Security	268
mac-learning	268
port security	269
show port security	271
Network Access (MAC Address Authentication)	273
network-access aging	273
network-access mac-filter	274
mac-authentication reauth-time	275
network-access dynamic-qos	276
network-access dynamic-vlan	277
network-access guest-vlan	278
network-access max-mac-count	278
network-access mode mac-authentication	279
network-access port-mac-filter	280
mac-authentication intrusion-action	281
mac-authentication max-mac-count	281
clear network-access	282
show network-access	282
show network-access mac-address-table	283
show network-access mac-filter	284
Web Authentication	284
web-auth login-attempts	285
web-auth quiet-period	286
web-auth session-timeout	286
web-auth system-auth-control	287
web-auth	287
web-auth re-authenticate (Port)	288
web-auth re-authenticate (IP)	288
show web-auth	289
show web-auth interface	289
show web-auth summary	290

DHCPv4 Snooping	290
ip dhcp snooping	291
ip dhcp snooping information option	293
ip dhcp snooping information option encode no-subtype	294
ip dhcp snooping information option remote-id	296
ip dhcp snooping information option tr101 board-id	297
ip dhcp snooping information policy	297
ip dhcp snooping verify mac-address	298
ip dhcp snooping vlan	299
ip dhcp snooping information option circuit-id	300
ip dhcp snooping max-number	301
ip dhcp snooping trust	302
clear ip dhcp snooping binding	303
clear ip dhcp snooping database flash	303
ip dhcp snooping database flash	303
show ip dhcp snooping	304
show ip dhcp snooping binding	304
DHCPv6 Snooping	305
ipv6 dhcp snooping	305
ipv6 dhcp snooping option remote-id	308
ipv6 dhcp snooping option remote-id policy	309
ipv6 dhcp snooping vlan	310
ipv6 dhcp snooping max-binding	311
ipv6 dhcp snooping trust	311
clear ipv6 dhcp snooping binding	312
clear ipv6 dhcp snooping statistics	313
show ipv6 dhcp snooping	313
show ipv6 dhcp snooping binding	313
show ipv6 dhcp snooping statistics	314
IPv4 Source Guard	314
ip source-guard binding	315
ip source-guard	317
ip source-guard max-binding	318
ip source-guard mode	319
clear ip source-guard binding blocked	320

show ip source-guard	320
show ip source-guard binding	321
IPv6 Source Guard	322
ipv6 source-guard binding	322
ipv6 source-guard	324
ipv6 source-guard max-binding	325
show ipv6 source-guard	326
show ipv6 source-guard binding	327
ARP Inspection	327
ip arp inspection	328
ip arp inspection filter	329
ip arp inspection log-buffer logs	330
ip arp inspection validate	331
ip arp inspection vlan	332
ip arp inspection limit	333
ip arp inspection trust	333
show ip arp inspection configuration	334
show ip arp inspection interface	334
show ip arp inspection log	335
show ip arp inspection statistics	335
show ip arp inspection vlan	335
Denial of Service Protection	336
dos-protection echo-charge	337
dos-protection smurf	337
dos-protection tcp-flooding	338
dos-protection tcp-null-scan	338
dos-protection tcp-syn-fin-scan	339
dos-protection tcp-xmas-scan	339
dos-protection udp-flooding	340
dos-protection win-nuke	340
show dos-protection	341
Port-based Traffic Segmentation	341
traffic-segmentation	342
traffic-segmentation session	343
traffic-segmentation uplink/downlink	343



traffic-segmentation uplink-to-uplink	344
show traffic-segmentation	345
<b>10 Access Control Lists</b>	<b>347</b>
IPv4 ACLs	347
access-list ip	348
permit, deny (Standard IP ACL)	348
permit, deny (Extended IPv4 ACL)	349
ip access-group	352
show ip access-group	353
show ip access-list	353
IPv6 ACLs	354
access-list ipv6	354
permit, deny (Standard IPv6 ACL)	355
permit, deny (Extended IPv6 ACL)	356
ipv6 access-group	359
show ipv6 access-group	359
show ipv6 access-list	360
MAC ACLs	360
access-list mac	361
permit, deny (MAC ACL)	361
mac access-group	364
show mac access-group	365
show mac access-list	365
ARP ACLs	366
access-list arp	366
permit, deny (ARP ACL)	367
show access-list arp	368
ACL Information	368
clear access-list hardware counters	369
show access-group	369
show access-list	370
<b>11 Interface Commands</b>	<b>371</b>
Interface Configuration	372
interface	372

capabilities	373
description	374
discard	375
flowcontrol	375
history	376
media-type	377
negotiation	377
shutdown	378
speed-duplex	379
clear counters	380
show interfaces brief	381
show interfaces counters	381
show interfaces history	385
show interfaces status	387
show interfaces switchport	388
Transceiver Threshold Configuration	389
transceiver-monitor	389
transceiver-threshold-auto	390
transceiver-threshold current	390
transceiver-threshold rx-power	391
transceiver-threshold temperature	392
transceiver-threshold tx-power	393
transceiver-threshold voltage	394
show interfaces transceiver	395
show interfaces transceiver-threshold	396
Cable Diagnostics	397
test cable-diagnostics	397
show cable-diagnostics	398
Power Savings	399
power-save	399
show power-save	400
<b>12 Link Aggregation Commands</b>	<b>401</b>
Manual Configuration Commands	402
port channel load-balance	402

channel-group	404
Dynamic Configuration Commands	405
lacp	405
lacp admin-key (Ethernet Interface)	406
lacp port-priority	407
lacp system-priority	408
lacp admin-key (Port Channel)	409
lacp timeout	410
Trunk Status Display Commands	411
show lacp	411
show port-channel load-balance	414
<b>13 Port Mirroring Commands</b>	<b>415</b>
Local Port Mirroring Commands	415
port monitor	415
show port monitor	417
RSPAN Mirroring Commands	418
rspan source	420
rspan destination	421
rspan remote vlan	422
no rspan session	423
show rspan	424
<b>14 Congestion Control Commands</b>	<b>425</b>
Rate Limit Commands	425
rate-limit	426
Storm Control Commands	427
switchport packet-rate	427
<b>15 Loopback Detection Commands</b>	<b>429</b>
loopback-detection	430
loopback-detection action	430
loopback-detection recover-time	431
loopback-detection transmit-interval	432
loopback detection trap	432
loopback-detection release	433

show loopback-detection	434
<b>16 Address Table Commands</b>	<b>435</b>
mac-address-table aging-time	435
mac-address-table static	436
clear collision-mac-address-table	437
clear mac-address-table dynamic	437
show collision-mac-address-table	437
show mac-address-table	438
show mac-address-table aging-time	439
show mac-address-table count	439
<b>17 Spanning Tree Commands</b>	<b>441</b>
spanning-tree	442
spanning-tree cisco-prestandard	443
spanning-tree forward-time	444
spanning-tree hello-time	444
spanning-tree max-age	445
spanning-tree mode	446
spanning-tree mst configuration	447
spanning-tree pathcost method	447
spanning-tree priority	448
spanning-tree system-bpdu-flooding	449
spanning-tree tc-prop	449
spanning-tree transmission-limit	450
max-hops	451
mst priority	451
mst vlan	452
name	453
revision	453
spanning-tree bpdu-filter	454
spanning-tree bpdu-guard	455
spanning-tree cost	456
spanning-tree edge-port	457
spanning-tree link-type	458
spanning-tree loopback-detection	458

spanning-tree loopback-detection action	459
spanning-tree loopback-detection release-mode	460
spanning-tree loopback-detection trap	461
spanning-tree restricted-tcn	461
spanning-tree mst cost	462
spanning-tree mst port-priority	463
spanning-tree port-bpdu-flooding	463
spanning-tree port-priority	464
spanning-tree root-guard	465
spanning-tree spanning-disabled	466
spanning-tree tc-prop-stop	466
spanning-tree loopback-detection release	467
spanning-tree protocol-migration	467
show spanning-tree	468
show spanning-tree mst configuration	470
show spanning-tree tc-prop	471
<b>18 VLAN Commands</b>	<b>473</b>
GVRP and Bridge Extension Commands	474
bridge-ext gvrp	474
garp timer	475
switchport forbidden vlan	476
switchport gvrp	476
show bridge-ext	477
show garp timer	478
show gvrp configuration	479
Editing VLAN Groups	479
vlan database	479
vlan	480
Configuring VLAN Interfaces	481
interface vlan	482
switchport acceptable-frame-types	483
switchport allowed vlan	483
switchport ingress-filtering	485
switchport mode	485

switchport native vlan	486
Displaying VLAN Information	487
show vlan	487
Configuring IEEE 802.1Q Tunneling	488
dot1q-tunnel system-tunnel-control	489
switchport dot1q-tunnel mode	490
switchport dot1q-tunnel priority map	491
switchport dot1q-tunnel service default match all discard	491
switchport dot1q-tunnel service default match untagged discard	492
switchport dot1q-tunnel service match cvid	492
switchport dot1q-tunnel tpid	495
show dot1q-tunnel service	496
show dot1q-tunnel	497
Configuring L2PT Tunneling	498
l2protocol-tunnel tunnel-dmac	498
switchport l2protocol-tunnel	501
show l2protocol-tunnel	502
Configuring VLAN Translation	502
switchport vlan-translation	502
show vlan-translation	504
Configuring Protocol-based VLANs	504
protocol-vlan protocol-group (Configuring Groups)	505
protocol-vlan protocol-group (Configuring Interfaces)	506
show protocol-vlan protocol-group	507
show interfaces protocol-vlan protocol-group	508
Configuring IP Subnet VLANs	508
subnet-vlan	509
show subnet-vlan	510
Configuring MAC Based VLANs	510
mac-vlan	511
show mac-vlan	512
Configuring Voice VLANs	512
voice vlan	513
voice vlan aging	514
voice vlan mac-address	515

switchport voice vlan	516
switchport voice vlan priority	516
switchport voice vlan rule	517
switchport voice vlan security	518
show voice vlan	518
<b>19 ERPS Commands</b>	<b>521</b>
erps	523
erps domain	524
control-vlan	524
enable	525
guard-timer	526
holdoff-timer	527
major-domain	527
meg-level	528
mep-monitor	529
node-id	530
non-erps-dev-protect	530
non-revertive	532
propagate-tc	535
raps-def-mac	536
raps-without-vc	537
ring-port	539
rpl neighbor	540
rpl owner	540
version	541
wtr-timer	542
clear erps statistics	543
erps clear	543
erps forced-switch	544
erps manual-switch	546
show erps	547
<b>20 Class of Service Commands</b>	<b>553</b>
Priority Commands (Layer 2)	553
queue mode	554

queue weight	555
switchport priority default	556
show queue mode	557
show queue weight	557
Priority Commands (Layer 3 and 4)	558
qos map cos-queue	558
qos map dscp-queue	560
qos map trust-mode	561
show qos map cos-queue	562
show qos map dscp-queue	563
show qos map trust-mode	563
<b>21 Quality of Service Commands</b>	<b>565</b>
class-map	566
description	567
match	568
rename	569
policy-map	570
class	570
police rate	571
set cos	572
set ip dscp	573
service-policy	574
show class-map	574
show policy-map	575
show policy-map interface	576
<b>22 Multicast Filtering Commands</b>	<b>577</b>
IGMP Snooping	577
ip igmp snooping	579
ip igmp snooping priority	580
ip igmp snooping proxy-reporting	580
ip igmp snooping querier	581
ip igmp snooping router-alert-option-check	582
ip igmp snooping router-port-expire-time	582
ip igmp snooping tcn-flood	583



ip igmp snooping tcn-query-solicit	584
ip igmp snooping unregistered-data-flood	585
ip igmp snooping unsolicited-report-interval	585
ip igmp snooping version	586
ip igmp snooping version-exclusive	587
ip igmp snooping vlan general-query-suppression	587
ip igmp snooping vlan immediate-leave	588
ip igmp snooping vlan last-memb-query-count	589
ip igmp snooping vlan last-memb-query-intvl	590
ip igmp snooping vlan mrd	590
ip igmp snooping vlan proxy-address	591
ip igmp snooping vlan query-interval	593
ip igmp snooping vlan query-resp-intvl	593
ip igmp snooping vlan static	594
clear ip igmp snooping groups dynamic	595
clear ip igmp snooping statistics	595
show ip igmp snooping	596
show ip igmp snooping group	597
show ip igmp snooping mrouter	598
show ip igmp snooping statistics	598
Static Multicast Routing	601
ip igmp snooping vlan mrouter	601
IGMP Filtering and Throttling	602
ip igmp filter (Global Configuration)	603
ip igmp profile	604
permit, deny	604
range	605
ip igmp authentication	605
ip igmp filter (Interface Configuration)	607
ip igmp max-groups	608
ip igmp max-groups action	608
ip igmp query-drop	609
ip multicast-data-drop	609
show ip igmp authentication	610
show ip igmp filter	611

show ip igmp profile	611
show ip igmp query-drop	612
show ip igmp throttle interface	612
show ip multicast-data-drop	613
MLD Snooping	614
ipv6 mld snooping	615
ipv6 mld snooping proxy-reporting	615
ipv6 mld snooping querier	616
ipv6 mld snooping query-interval	617
ipv6 mld snooping query-max-response-time	617
ipv6 mld snooping robustness	618
ipv6 mld snooping router-port-expire-time	618
ipv6 mld snooping unknown-multicast mode	619
ipv6 mld snooping unsolicited-report-interval	620
ipv6 mld snooping version	620
ipv6 mld snooping vlan immediate-leave	621
ipv6 mld snooping vlan mrouter	622
ipv6 mld snooping vlan static	623
clear ipv6 mld snooping groups dynamic	623
clear ipv6 mld snooping statistics	624
show ipv6 mld snooping	624
show ipv6 mld snooping group	625
show ipv6 mld snooping group source-list	625
show ipv6 mld snooping mrouter	626
show ipv6 mld snooping statistics	627
MLD Filtering and Throttling	631
ipv6 mld filter (Global Configuration)	631
ipv6 mld profile	632
permit, deny	633
range	633
ipv6 mld filter (Interface Configuration)	634
ipv6 mld max-groups	635
ipv6 mld max-groups action	635
ipv6 mld query-drop	636
ipv6 multicast-data-drop	636

show ipv6 mld filter	637
show ipv6 mld profile	638
show ipv6 mld query-drop	638
show ipv6 mld throttle interface	639
MVR for IPv4	640
mvr	641
mvr associated-profile	641
mvr domain	642
mvr priority	643
mvr profile	643
mvr proxy-query-interval	644
mvr proxy-switching	645
mvr robustness-value	646
mvr source-port-mode dynamic	647
mvr upstream-source-ip	647
mvr vlan	648
mvr immediate-leave	649
mvr type	650
mvr vlan group	651
clear mvr groups dynamic	652
clear mvr statistics	652
show mvr	653
show mvr associated-profile	654
show mvr interface	654
show mvr members	655
show mvr profile	657
show mvr statistics	658
MVR for IPv6	662
mvr6 associated-profile	663
mvr6 domain	663
mvr6 priority	664
mvr6 profile	665
mvr6 proxy-query-interval	666
mvr6 proxy-switching	666
mvr6 robustness-value	667

mvr6 source-port-mode dynamic	668
mvr6 upstream-source-ip	669
mvr6 vlan	669
mvr6 immediate-leave	670
mvr6 type	671
mvr6 vlan group	672
clear mvr6 groups dynamic	673
clear mvr6 statistics	674
show mvr6	674
show mvr6 associated-profile	675
show mvr6 interface	676
show mvr6 members	677
show mvr6 profile	678
show mvr6 statistics	679
<b>23 LLDP Commands</b>	<b>681</b>
lldp	683
lldp holdtime-multiplier	683
lldp med-fast-start-count	684
lldp notification-interval	684
lldp refresh-interval	685
lldp reinit-delay	685
lldp tx-delay	686
lldp admin-status	687
lldp basic-tlv management-ip-address	687
lldp basic-tlv port-description	688
lldp basic-tlv system-capabilities	688
lldp basic-tlv system-description	689
lldp basic-tlv system-name	689
lldp dot1-tlv proto-ident	690
lldp dot1-tlv proto-vid	690
lldp dot1-tlv pvid	691
lldp dot1-tlv vlan-name	691
lldp dot3-tlv link-agg	692
lldp dot3-tlv mac-phy	692

lldp dot3-tlv max-frame	693
lldp med-location civic-addr	694
lldp med-notification	695
lldp med-tlv inventory	696
lldp med-tlv location	697
lldp med-tlv med-cap	697
lldp med-tlv network-policy	698
lldp notification	698
show lldp config	699
show lldp info local-device	700
show lldp info remote-device	701
show lldp info statistics	703
<b>24 CFM Commands</b>	<b>705</b>
Defining CFM Structures	708
ethernet cfm ais level	708
ethernet cfm ais ma	709
ethernet cfm ais period	710
ethernet cfm ais suppress alarm	710
ethernet cfm domain	711
ethernet cfm enable	713
ma index name	714
ma index name-format	715
ethernet cfm mep	716
ethernet cfm port-enable	717
clear ethernet cfm ais mpid	717
show ethernet cfm configuration	718
show ethernet cfm md	720
show ethernet cfm ma	720
show ethernet cfm maintenance-points local	721
show ethernet cfm maintenance-points local detail mep	722
show ethernet cfm maintenance-points remote detail	723
Continuity Check Operations	725
ethernet cfm cc ma interval	725
ethernet cfm cc enable	726

snmp-server enable traps ethernet cfm cc	727
mep archive-hold-time	728
clear ethernet cfm maintenance-points remote	728
clear ethernet cfm errors	729
show ethernet cfm errors	730
Cross Check Operations	731
ethernet cfm mep crosscheck start-delay	731
snmp-server enable traps ethernet cfm crosscheck	731
mep crosscheck mpid	732
ethernet cfm mep crosscheck	733
show ethernet cfm maintenance-points remote crosscheck	734
Link Trace Operations	734
ethernet cfm linktrace cache	734
ethernet cfm linktrace cache hold-time	735
ethernet cfm linktrace cache size	736
ethernet cfm linktrace	736
clear ethernet cfm linktrace-cache	738
show ethernet cfm linktrace-cache	738
Loopback Operations	739
ethernet cfm loopback	739
Fault Generator Operations	740
mep fault-notify alarm-time	740
mep fault-notify lowest-priority	741
mep fault-notify reset-time	742
show ethernet cfm fault-notify-generator	743
Delay Measure Operations	744
ethernet cfm delay-measure two-way	744
<b>25 OAM Commands</b>	<b>747</b>
efm oam	748
efm oam critical-link-event	748
efm oam link-monitor frame	749
efm oam link-monitor frame threshold	750
efm oam link-monitor frame window	750
efm oam mode	<b>751</b>

clear efm oam counters	752
clear efm oam event-log	752
efm oam remote-loopback	753
efm oam remote-loopback test	754
show efm oam counters interface	755
show efm oam event-log interface	755
show efm oam remote-loopback interface	757
show efm oam status interface	757
show efm oam status remote interface	758
<b>26 Domain Name Service Commands</b>	<b>759</b>
DNS Commands	760
ip domain-list	760
ip domain-lookup	761
ip domain-name	762
ip host	762
ip name-server	763
ipv6 host	764
clear dns cache	765
clear host	765
show dns	766
show dns cache	766
show hosts	767
Multicast DNS Commands	767
ip mdns	767
show ip mdns	768
<b>27 DHCP Commands</b>	<b>769</b>
DHCP Client	769
DHCP for IPv4	770
ip dhcp dynamic-provision	770
ip dhcp client class-id	771
ip dhcp restart client	773
show ip dhcp dynamic-provision	773
DHCP for IPv6	774
ipv6 dhcp client rapid-commit vlan	774

ipv6 dhcp restart client vlan	774
show ipv6 dhcp duid	776
show ipv6 dhcp vlan	776
DHCP Relay	777
ip dhcp relay server	777
ip dhcp restart relay	778
<b>28 IP Interface Commands</b>	<b>781</b>
IPv4 Interface	781
Basic IPv4 Configuration	782
ip address	782
ip default-gateway	784
show ip default-gateway	785
show ip interface	785
show ip traffic	786
traceroute	787
ping	788
ARP Configuration	789
arp	789
ip proxy-arp	790
clear arp-cache	791
show arp	791
IPv6 Interface	792
Interface Address Configuration and Utilities	793
ipv6 default-gateway	793
ipv6 address	794
ipv6 address autoconfig	795
ipv6 address eui-64	797
ipv6 address link-local	799
ipv6 enable	800
ipv6 mtu	801
show ipv6 default-gateway	802
show ipv6 interface	802
show ipv6 mtu	805
show ipv6 traffic	805



clear ipv6 traffic	810
ping6	810
traceroute6	811
Neighbor Discovery	812
clear ipv6 neighbors	812
show ipv6 neighbors	813
<b>28 IP Routing Commands</b>	<b>815</b>
Global Routing Configuration	815
IPv4 Commands	816
ip route	816
show ip route	817

---

<b>Section III</b>	<b>Appendices</b>	<b>819</b>
<b>A</b>	<b>Troubleshooting</b>	<b>821</b>
	Problems Accessing the Management Interface	821
	Using System Logs	822
<b>B</b>	<b>License Information</b>	<b>823</b>
	The GNU General Public License	823
	<b>Glossary</b>	<b>827</b>
	<b>List of Commands</b>	<b>835</b>
	<b>Index</b>	<b>843</b>



---

# Tables

Table 1: Options 60, 66 and 67 Statements	63
Table 2: Options 55 and 124 Statements	63
Table 3: General Command Modes	75
Table 4: Configuration Command Modes	77
Table 5: Keystroke Commands	77
Table 6: Command Group Index	79
Table 7: General Commands	81
Table 8: System Management Commands	89
Table 9: Device Designation Commands	89
Table 10: System Status Commands	90
Table 11: show access-list tcam-utilization - display description	92
Table 12: show process cpu guard - display description	94
Table 13: show system – display description	98
Table 14: show version – display description	101
Table 15: Frame Size Commands	102
Table 16: Flash/File Commands	104
Table 17: File Directory Information	110
Table 18: Line Commands	116
Table 19: Event Logging Commands	127
Table 20: Logging Levels	129
Table 21: show logging flash/ram - display description	133
Table 22: show logging trap - display description	134
Table 23: Event Logging Commands	134
Table 24: Time Commands	138
Table 25: Predefined Summer-Time Parameters	147
Table 26: Time Range Commands	151
Table 27: Switch Cluster Commands	154
Table 28: SNMP Commands	161
Table 29: show snmp engine-id - display description	176

Table 30: show snmp group - display description	177
Table 31: show snmp user - display description	178
Table 32: show snmp view - display description	179
Table 33: RMON Commands	187
Table 34: sFlow Commands	195
Table 35: Authentication Commands	201
Table 36: User Access Commands	202
Table 37: Default Login Settings	204
Table 38: Authentication Sequence Commands	206
Table 39: RADIUS Client Commands	208
Table 40: TACACS+ Client Commands	212
Table 41: AAA Commands	216
Table 42: Web Server Commands	228
Table 43: HTTPS System Support	232
Table 44: Telnet Server Commands	232
Table 45: Secure Shell Commands	235
Table 46: show ssh - display description	244
Table 47: 802.1X Port Authentication Commands	245
Table 48: Management IP Filter Commands	257
Table 49: PPPoE Intermediate Agent Commands	259
Table 50: show pppoe intermediate-agent statistics - display description	266
Table 51: General Security Commands	267
Table 52: Management IP Filter Commands	268
Table 53: show port security - display description	271
Table 54: Network Access Commands	273
Table 55: Dynamic QoS Profiles	276
Table 56: Web Authentication	285
Table 57: DHCP Snooping Commands	290
Table 58: Option 82 information	295
Table 59: Option 82 information	300
Table 60: DHCP Snooping Commands	305
Table 61: IPv4 Source Guard Commands	314
Table 62: IPv6 Source Guard Commands	322
Table 63: ARP Inspection Commands	327
Table 64: DoS Protection Commands	336

Table 65: Commands for Configuring Traffic Segmentation	341
Table 66: Traffic Segmentation Forwarding	342
Table 67: Access Control List Commands	347
Table 68: IPv4 ACL Commands	347
Table 69: IPv6 ACL Commands	354
Table 70: MAC ACL Commands	360
Table 71: ARP ACL Commands	366
Table 72: ACL Information Commands	368
Table 73: Interface Commands	371
Table 74: show interfaces counters - display description	383
Table 75: show interfaces switchport - display description	388
Table 76: Link Aggregation Commands	401
Table 77: show lacp counters - display description	411
Table 78: show lacp internal - display description	412
Table 79: show lacp neighbors - display description	413
Table 80: show lacp sysid - display description	414
Table 81: Port Mirroring Commands	415
Table 82: Mirror Port Commands	415
Table 83: RSPAN Commands	418
Table 84: Congestion Control Commands	425
Table 85: Rate Limit Commands	425
Table 86: Rate Limit Commands	427
Table 87: Loopback Detection Commands	429
Table 88: Address Table Commands	435
Table 89: Spanning Tree Commands	441
Table 90: Recommended STA Path Cost Range	456
Table 91: Default STA Path Costs	456
Table 92: VLAN Commands	473
Table 93: GVRP and Bridge Extension Commands	474
Table 94: show bridge-ext - display description	477
Table 95: Commands for Editing VLAN Groups	479
Table 96: Commands for Configuring VLAN Interfaces	481
Table 97: Commands for Displaying VLAN Information	487
Table 98: 802.1Q Tunneling Commands	488
Table 99: L2 Protocol Tunnel Commands	498

Table 100: VLAN Translation Commands	502
Table 101: Protocol-based VLAN Commands	505
Table 102: IP Subnet VLAN Commands	508
Table 103: MAC Based VLAN Commands	510
Table 104: Voice VLAN Commands	512
Table 105: ERPS Commands	521
Table 106: ERPS Request/State Priority	545
Table 107: show erps - summary display description	548
Table 108: show erps domain - detailed display description	549
Table 109: show erps statistics - detailed display description	551
Table 110: Priority Commands	553
Table 111: Priority Commands (Layer 2)	553
Table 112: Priority Commands (Layer 3 and 4)	558
Table 113: Default Mapping of CoS/CFI Values to Queue/CFI	559
Table 114: Default Mapping of DSCP/CFI Values to Queue	560
Table 115: Quality of Service Commands	565
Table 116: Multicast Filtering Commands	577
Table 117: IGMP Snooping Commands	577
Table 118: show ip igmp snooping statistics input - display description	599
Table 119: show ip igmp snooping statistics output - display description	599
Table 120: show ip igmp snooping statistics vlan query - display description	600
Table 121: Static Multicast Interface Commands	601
Table 122: IGMP Filtering and Throttling Commands	602
Table 123: IGMP Authentication RADIUS Attribute Value Pairs	606
Table 124: MLD Snooping Commands	614
Table 125: show ipv6 MLD snooping statistics input - display description	627
Table 126: show ipv6 MLD snooping statistics output - display description	628
Table 127: show ipv6 MLD snooping statistics query - display description	629
Table 128: show ipv6 MLD snooping statistics summary - display description	630
Table 129: MLD Filtering and Throttling Commands	631
Table 130: Multicast VLAN Registration for IPv4 Commands	640
Table 131: show mvr - display description	653
Table 132: show mvr interface - display description	655
Table 133: show mvr members - display description	657
Table 134: show mvr statistics input - display description	658

Table 135: show mvr statistics output - display description	659
Table 136: show mvr statistics query - display description	660
Table 137: show mvr statistics summary interface - display description	661
Table 138: Multicast VLAN Registration for IPv6 Commands	662
Table 139: show mvr6 - display description	675
Table 140: show mvr6 interface - display description	676
Table 141: show mvr6 members - display description	678
Table 142: show mvr6 statistics input - display description	679
Table 143: show mvr6 statistics output - display description	680
Table 144: LLDP Commands	681
Table 145: LLDP MED Location CA Types	694
Table 146: CFM Commands	705
Table 147: show ethernet cfm configuration traps - display description	719
Table 148: show ethernet cfm maintenance-points local detail mep - display	723
Table 149: show ethernet cfm maintenance-points remote detail - display	724
Table 150: show ethernet cfm errors - display description	730
Table 151: show ethernet cfm linktrace-cache - display description	738
Table 152: Remote MEP Priority Levels	742
Table 153: MEP Defect Descriptions	742
Table 154: show fault-notify-generator - display description	743
Table 155: OAM Commands	747
Table 156: Address Table Commands	759
Table 157: show dns cache - display description	766
Table 158: show hosts - display description	767
Table 159: DHCP Commands	769
Table 160: DHCP Client Commands	769
Table 161: Options 60, 66 and 67 Statements	772
Table 162: Options 55 and 124 Statements	772
Table 163: DHCP Relay Option 82 Commands	777
Table 164: IP Interface Commands	781
Table 165: IPv4 Interface Commands	781
Table 166: Basic IP Configuration Commands	782
Table 167: Address Resolution Protocol Commands	789
Table 168: IPv6 Configuration Commands	792
Table 169: show ipv6 interface - display description	803

Table 170: show ipv6 mtu - display description	805
Table 171: show ipv6 traffic - display description	806
Table 172: show ipv6 neighbors - display description	813
Table 160: IP Routing Commands	815
Table 161: Global Routing Configuration Commands	815
Table 162: Troubleshooting Chart	821



# 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 43](#)



# 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 47](#).

---

### 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
- ◆ Enable GVRP automatic VLAN registration
- ◆ 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 26)
- ◆ 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 RS-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 ECS4100-26TX* 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 ECS4100-26TX and ECS4100-26TX-ME 10 Gigabit Ethernet switches, and the ECS4100-28T and ECS4100-52T Gigabit Ethernet switches. Other than the difference in the number of ports, and the dual power input sources provided on the ECS4100-26TX-ME, 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 47](#).

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 47](#)) 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 (1-26/52).

**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 52](#).

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 48](#).

### 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 792](#).

**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): ECS4110-28
  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 such as Edge-Core ECView Pro. 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 161](#) 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 56](#) 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 128 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: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode: m360.bix
Console(config)#exit
Console#dir
File Name                               Type      Startup Modified Time          Size (bytes)
-----
Unit 1:
ECS4100_V1.1.3.164.bix                  OpCode   Y        2016-10-17 11:30:26     9027848
Factory_Default_Config.cfg              Config   N        2015-07-01 07:24:11         455
startup1.cfg                             Config   Y        2015-07-01 07:24:22         1343
-----
Free space for compressed user config files: 24043520
Total space:                               32 MB
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 ECS4100-series.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 *ECS4100-Series.BIX* from the server even though *ECS4100-series.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, *ecs4100\_series.bix* and *ECS4100\_Series.BIX* are considered to be unique files. Thus, if the upgrade file is stored as *ECS4100\_Series.BIX* (or even *Ecs4100\_Series.bix*) on a case-sensitive server, then the switch (requesting *ECS4100\_Series.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 ECS4100-series.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   : ECS4100-series.bix  
Console#
```

The following shows an example of the upgrade process.

```

Console#dir
      File Name                Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
ECS4100_V1.1.3.164.bix        OpCode Y      2016-10-17 11:30:26    9027848
Factory_Default_Config.cfg    Config  N      2015-04-13 13:55:58     455
startup1.cfg                  Config  Y      2015-07-13 04:03:49     1707
-----
Free space for compressed user config files: 1355776
Total space: 32 MB

...
Press ENTER to start session
Automatic Upgrade is looking for a new image
New image detected: current version V1.1.3.164; new version V1.1.3.165
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 ECS4100-26TX is opened.
      To end the CLI session, enter [Exit].

Console#dir
      File Name                Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
ECS4100_V1.1.3.165.bix        OpCode Y      2016-10-17 11:30:26    9027848
Factory_Default_Config.cfg    Config  N      2015-04-13 13:55:58     455
startup1.cfg                  Config  Y      2015-07-13 04:03:49     1707
-----
Free space for compressed user config files: 1310720
Total space: 32 MB

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 = "ecs4100-26tx.cfg";
    option tftp-server-name "192.168.255.101";
    option bootfile-name "test";
}
```



**Note:** Use "ecs4100-26tx.cfg" 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 bootup.

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 14:11:36, April 1st, 2013, enter this command.

```
Console#calendar set 14 11 36 1 April 2013
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 69](#)
- ◆ ["General Commands" on page 81](#)
- ◆ ["System Management Commands" on page 89](#)
- ◆ ["SNMP Commands" on page 161](#)
- ◆ ["Remote Monitoring Commands" on page 187](#)
- ◆ ["Flow Sampling Commands" on page 195](#)
- ◆ ["Authentication Commands" on page 201](#)
- ◆ ["General Security Measures" on page 267](#)
- ◆ ["Access Control Lists" on page 347](#)
- ◆ ["Interface Commands" on page 371](#)
- ◆ ["Link Aggregation Commands" on page 401](#)
- ◆ ["Port Mirroring Commands" on page 415](#)
- ◆ ["Congestion Control Commands" on page 425](#)
- ◆ ["Loopback Detection Commands" on page 429](#)
- ◆ ["Address Table Commands" on page 435](#)
- ◆ ["Spanning Tree Commands" on page 441](#)

- ◆ “VLAN Commands” on page 473
- ◆ “ERPS Commands” on page 521
- ◆ “Class of Service Commands” on page 553
- ◆ “Quality of Service Commands” on page 565
- ◆ “Multicast Filtering Commands” on page 577
- ◆ “LLDP Commands” on page 681
- ◆ “CFM Commands” on page 705
- ◆ “OAM Commands” on page 747
- ◆ “Domain Name Service Commands” on page 759
- ◆ “DHCP Commands” on page 769
- ◆ “IP Interface Commands” on page 781
- ◆ “IP Routing Commands” on page 815

# 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 ECS4100-26TX 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 ECS4100-26TX 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 system ?**” 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
debug            State of each debugging option
discard          Discard packet
dns              DNS information
dos-protection   Shows the system dos-protection summary information
dot1q-tunnel     802.1Q tunnel
dot1x            802.1X content
efm              Ethernet First Mile feature
erps             Displays ERPS configuration
ethernet         Shows Metro Ethernet information
garp            GARP properties
gvrp            GVRP interface information
history         Shows history information
hosts           Host information
interfaces      Shows interface information
ip             IP information
ipv6           IPv6 information
l2protocol-tunnel Layer 2 protocol tunneling configuration
lACP           LACP statistics
license        Show license
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
mvr         multicast VLAN registration
mvr6        IPv6 Multicast VLAN registration
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-save  Shows the power saving information
pppoe       Displays PPPoE configuration
```



```
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
sntp              Simple Network Time Protocol configuration
spanning-tree     Spanning-tree configuration
ssh               Secure shell server connections
startup-config    Startup system configuration
subnet-vlan       IP subnet-based VLAN information
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#show
```

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 subnet-vlan    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 ECS4100-26TX is opened.
To end the CLI session, enter [Exit].

Console#

```

```

Username: guest
Password: [guest login password]

CLI session with the ECS4100-26TX 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.
- ◆ DHCP Configuration - These commands are used to configure the DHCP server.
- ◆ 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)	366
	access-list ip standard	Console(config-std-acl)	348
	access-list ip extended	Console(config-ext-acl)	348
	access-list ipv6 standard	Console(config-std-ipv6-acl)	354
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	354
	access-list mac	Console(config-mac-acl)	361
Class Map	class-map	Console(config-cmap)	566
Interface	interface {ethernet <i>port</i>   port-channel <i>id</i>   vlan <i>id</i> }	Console(config-if)	372
Line	line {console   vty}	Console(config-line)	117
MSTP	spanning-tree mst-configuration	Console(config-mstp)	447
Policy Map	policy-map	Console(config-pmap)	570
Time Range	time-range	Console(config-time-range)	151
VLAN	vlan database	Console(config-vlan)	479

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.

**Table 5: Keystroke Commands** (Continued)

Keystroke	Function
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	81
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, the system clock, and switch clustering	89
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	161
Remote Monitoring	Supports statistics, history, alarm and event groups	187
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	201
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	267
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)	347
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	371
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	401
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	415
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.	425
Loopback Detection	Detects general loopback conditions caused by hardware problems or faulty protocol settings	429
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	435
Spanning Tree	Configures Spanning Tree settings for the switch	441
ERPS	Configures Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks	521

**Table 6: Command Group Index** (Continued)

<b>Command Group</b>	<b>Description</b>	<b>Page</b>
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	<a href="#">473</a>
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	<a href="#">553</a>
Quality of Service	Configures Differentiated Services	<a href="#">565</a>
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	<a href="#">577</a>
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	<a href="#">681</a>
Connectivity Fault Management	Configures connectivity monitoring using continuity check messages, fault verification through loopback messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices	<a href="#">705</a>
OAM	Configures Operations, Administration and Maintenance remote management tools required to monitor and maintain the links to subscriber CPEs	<a href="#">747</a>
Domain Name Service	Configures DNS services.	<a href="#">759</a>
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	<a href="#">769</a>
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters	<a href="#">781</a>
IP Routing	Configures static and dynamic unicast routing	<a href="#">815</a>
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)
- CFM** (Connectivity Fault Management Configuration)
- CM** (Class Map Configuration)
- ERPS** (Ethernet Ring Protection Switching 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: 255 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 105](#)).

**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 74](#).

**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 \(86\)](#)

[enable password \(202\)](#)

**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 74](#).

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```

Console#configure
Console(config)#

```

**Related Commands**

[end \(87\)](#)

**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 74](#).

**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 \(83\)](#)

**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
<a href="#">show access-list</a> <a href="#">tcam-utilization</a>	Shows utilization parameters for TCAM	PE
<a href="#">show memory</a>	Shows memory utilization parameters	PE
<a href="#">show process cpu</a>	Shows CPU utilization parameters	PE
<a href="#">show process cpu guard</a>	Shows the CPU utilization watermark and threshold	NE
<a href="#">show process cpu task</a>	Shows CPU utilization per process	PE
<a href="#">show running-config</a>	Displays the configuration data currently in use	PE
<a href="#">show startup-config</a>	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
<a href="#">show system</a>	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 tcam-utilization** This command shows utilization parameters for TCAM (Ternary Content 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,
I - IP source guard, C - CPU interface, L - Link local,
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 IPSV
1	0	6	128	0	128	DM
1	0	7	128	0	128	MV PV VV
1	0	8	64	0	64	I
1	0	9	64	0	64	I6
1	0	10	64	64	0	C
1	0	11	64	64	0	C L

```

1      0  12   64   0   64 AE6S AE6E
1      0  13  128   0  128 AE4
1      0  14  128   0  128 AEM
1      0  15   64   0   64 DE6S DE6E
1      0  16  128   0  128 DE4
1      0  17  128   0  128 DEM
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 \(182\)](#)

**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 \(183\)](#)

**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 \(184\)](#)

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

**Command Mode**

Privileged Exec

**Example**

```

Console#show process cpu task
Task          Util (%) Avg (%) Max (%)
-----
AMTR_ADDRESS  0.00    0.00  0.00
AMTRL3        0.00    0.00  0.00
AMTRL3_GROUP  0.00    0.00  0.00
APP_PROTOCOL_PR 0.00    0.00  0.00
AUTH_GROUP    0.00    0.00  0.00
AUTH_PROC     0.00    0.00  0.00
BGP_TD        0.00    0.00  0.00
CFGDB_TD      0.00    0.00  0.00
CFM_GROUP     0.00    0.00  0.00
CLITASK0      0.00    0.00  0.00
CORE_UTIL_PROC 0.00    0.00  0.00
DHCPSPNP_GROUP 0.00    0.00  0.00
DOT1X_SUP_GROUP 0.00    0.00  0.00
DRIVER_GROUP  1.00    0.75  2.00
DRIVER_GROUP_FR 0.00    0.00  0.00
DRIVER_GROUP_TX 0.00    0.00  0.00

```

FS	0.00	0.00	0.00
HTTP_TD	0.00	0.00	5.00
HW_WTDOG_TD	0.00	0.00	0.00
IML_TX	0.00	0.00	0.00
IP_SERVICE_GROU	0.00	0.00	0.00
KEYGEN_TD	0.00	0.00	0.00
L2_L4_PROCESS	0.00	0.00	4.00
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
MSL_TD	0.00	0.00	0.00
NETACCESS_GROUP	0.00	0.00	0.00
NETACCESS_NMTR	0.00	0.25	2.00
NETCFG_GROUP	0.00	0.00	0.00
NETCFG_PROC	0.00	0.08	1.00
NIC	0.00	0.00	0.00
NMTRDRV	1.00	1.66	4.00
NSM_GROUP	0.00	0.00	0.00
NSM_PROC	0.00	0.00	0.00
NSM_TD	0.00	0.00	0.00
OSPF6_TD	0.00	0.00	0.00
OSPF_TD	0.00	0.00	0.00
PIM_GROUP	0.00	0.00	0.00
PIM_PROC	0.00	0.00	0.00
PIM_SM_TD	0.00	0.00	0.00
POE_PROC	0.00	0.00	0.00
RIP_TD	0.00	0.00	0.00
SNMP_GROUP	0.00	0.00	0.00
SNMP_TD	0.00	0.00	0.00
SSH_GROUP	0.00	0.00	0.00
SSH_TD	0.00	0.00	0.00
STA_GROUP	0.00	0.00	0.00
STKCTRL_GROUP	0.00	0.00	0.00
STKTPLG_GROUP	0.00	0.00	0.00
SWCTRL_GROUP	0.00	0.00	0.00
SWCTRL_TD	0.00	0.00	0.00
SWDRV_MONITOR	21.00	19.25	21.00
SYS_MGMT_PROC	0.00	0.00	0.00
SYSDRV	0.00	0.00	0.00
SYSLOG_TD	0.00	0.00	0.00
SYSMGMT_GROUP	0.00	0.00	0.00
SYSTEM	0.00	0.00	0.00
UDLD_GROUP	0.00	0.00	0.00
WTDG_PROC	0.00	0.00	0.00
XFER_GROUP	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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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 \(97\)](#)

**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 \(96\)](#)

**show system** This command displays system information.

### Default Setting

None

### Command Mode

Normal Exec, Privileged Exec

### Example

```
Console#show system
System Description : ECS4100-26TX
System OID String : 1.3.6.1.4.1.259.10.1.46.102
System Information
  System Up Time      : 0 days, 2 hours, 25 minutes, and 27.66 seconds
  System Name        :
  System Location    :
  System Contact     :
  MAC Address (Unit 1) : 00-E0-0C-00-00-FD
  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

System Temperature:
Unit 1
  Temperature 1: 41 degrees

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.

**Table 13: show system – display description** (Continued)

Parameter	Description
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

Normal Exec, 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 ECS2100-28T is opened.
      To end the CLI session, enter [Exit].

Vty-2#show tech-support

dir:
File Name                               Type   Startup Modified Time           Size (bytes)
-----
Unit 1:
ECS2000-28PP_V0.0.0.8.bix                OpCode Y    2015-07-01 07:26:54       7733512
Factory_Default_Config.cfg              Config N    2015-07-01 07:24:11         455
startup1.cfg                             Config Y    2015-07-01 07:24:22        1343
-----
Free space for compressed user config files: 24018944
Total space:                               32 MB

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      : EC1609000920
Hardware Version   : R0A
Number of Ports    : 26
Main Power Status  : Up
Role               : Master
Loader Version     : 1.0.0.4
Linux Kernel Version : 2.6.19
Operation Code Version : 1.1.3.164

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

Disabled

#### 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
<a href="#">jumbo frame</a>	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 \(98\)](#)

[show ipv6 mtu \(805\)](#)

---

## File Management

### Managing Firmware

Firmware can be uploaded and downloaded to or from an FTP/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** {**config** | **opcode**}: *filename*

**config**\* - Configuration file.

**opcode**\* - Run-time operation code.

*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 config: startup
Console(config)#
```

## Related Commands

[dir \(110\)](#)

[whichboot \(111\)](#)

**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 235.)

**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 name filename | https-certificate | public-key username [dsa | rsa]}
```

**file** - Keyword that allows you to delete a file.

**name** - Keyword indicating a file.

*filename* - Name of configuration file or code image.

**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 235.](#))

*username* - Name of an SSH user. (Range: 1-8 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 test2.cfg  
Console#
```

### Related Commands

[dir \(110\)](#)

[delete public-key \(240\)](#)

**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:
ECS4100_V1.1.3.164.bix                  OpCode   Y          2016-10-17 11:30:26      9027848
Factory_Default_Config.cfg              Config   N          2015-07-01 07:24:11      455
startup1.cfg                             Config   Y          2015-07-01 07:24:22      1343
-----
Free space for compressed user config files: 24018944
Total space:                               32 MB
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:
ECS4100_V1.1.3.164.bix                  OpCode   Y          2016-10-17 11:30:26      9027848
startup1.cfg                             Config   Y          2015-07-01 07:24:22      1343
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 ECS2100-series.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 bootup.

```
:
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 ECS2100-series.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   : ECS4100-series.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

**Table 18: Line Commands** (Continued)

Command	Function	Mode
<a href="#">terminal</a>	Configures terminal settings, including escape-character, line length, terminal type, and width	PE
<a href="#">show line</a>	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.

**vty** - 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 \(126\)](#)

[show users \(100\)](#)

**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 \(120\)](#)

**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 \(203\)](#)

[password \(121\)](#)

**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 \(119\)](#)

[password-thresh \(121\)](#)

**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 \(122\)](#)

**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 \(121\)](#)

**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 \(244\)](#)

[show users \(100\)](#)

**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.

**Table 19: Event Logging Commands**

Command	Function	Mode
<a href="#">logging command</a>	Stores CLI command execution records in syslog RAM and flash	GC
<a href="#">logging facility</a>	Sets the facility type for remote logging of syslog messages	GC
<a href="#">logging history</a>	Limits syslog messages saved to switch memory based on severity	GC
<a href="#">logging host</a>	Adds a syslog server host IP address that will receive logging messages	GC
<a href="#">logging on</a>	Controls logging of error messages	GC
<a href="#">logging trap</a>	Limits syslog messages saved to a remote server based on severity	GC
<a href="#">clear log</a>	Clears messages from the logging buffer	PE
<a href="#">show log</a>	Displays log messages	PE
<a href="#">show logging</a>	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 \(128\)](#)

[logging trap \(131\)](#)

[clear log \(131\)](#)

**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 128](#). 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 \(132\)](#)

**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 138](#)).

**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 <a href="#">logging on</a> command.
History Logging in Flash	The message level(s) reported based on the <a href="#">logging history</a> command.
History Logging in RAM	The message level(s) reported based on the <a href="#">logging history</a> 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 <a href="#">logging on</a> command.
<i>Remote Logging Configuration</i>	
Status	Shows if remote logging has been enabled via the <a href="#">logging trap</a> command.
Facility Type	The facility type for remote logging of syslog messages as specified in the <a href="#">logging facility</a> command.
Level Type	The severity threshold for syslog messages sent to a remote server as specified in the <a href="#">logging trap</a> command.

### Related Commands

[show logging sendmail \(138\)](#)

## SMTP Alerts

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

**Table 23: Event Logging Commands**

Command	Function	Mode
<a href="#">logging sendmail</a>	Enables SMTP event handling	GC
<a href="#">logging sendmail destination-email</a>	Email recipients of alert messages	GC
<a href="#">logging sendmail host</a>	SMTP servers to receive alert messages	GC
<a href="#">logging sendmail level</a>	Severity threshold used to trigger alert messages	GC
<a href="#">logging sendmail source-email</a>	Email address used for "From" field of alert messages	GC
<a href="#">show logging sendmail</a>	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

**logging sendmail level** *level*

**no logging sendmail level**

*level* - One of the system message levels ([page 128](#)). 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
-----
192.168.1.19

SMTP Minimum Severity Level: 7

SMTP Destination E-mail Addresses
-----
ted@this-company.com

SMTP Source E-mail Address: bill@this-company.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.

**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 \(140\)](#)

[sntp poll \(140\)](#)

[show sntp \(141\)](#)

**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 \(139\)](#)

**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 \(139\)](#)

[sntp poll \(140\)](#)

[show sntp \(141\)](#)

**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 \(142\)](#)

**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 \(142\)](#)

**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 \(139\)](#)

[ntp server \(144\)](#)

**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 \(143\)](#)

[show ntp \(145\)](#)

**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 \(141\)](#)

**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 \(141\)](#)

**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 \(141\)](#)

**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 \(141\)](#)

**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 15:12:34, February 1st, 2015.

```
Console#calendar set 15:12:34 1 February 2015
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
<a href="#">time-range</a>	Specifies the name of a time range, and enters time range configuration mode	GC
<a href="#">absolute</a>	Sets the absolute time range for the execution of a command	TR
<a href="#">periodic</a>	Sets the time range for the periodic execution of a command	TR
<a href="#">show time-range</a>	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 \(347\)](#)

**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
<a href="#">cluster</a>	Configures clustering on the switch	GC
<a href="#">cluster commander</a>	Configures the switch as a cluster Commander	GC
<a href="#">cluster ip-pool</a>	Sets the cluster IP address pool for Members	GC
<a href="#">cluster member</a>	Sets Candidate switches as cluster members	GC
<a href="#">rcommand</a>	Provides configuration access to Member switches	PE

**Table 27: Switch Cluster Commands** (Continued)

Command	Function	Mode
<a href="#">show cluster</a>	Displays the switch clustering status	PE
<a href="#">show cluster members</a>	Displays current cluster Members	PE
<a href="#">show cluster candidates</a>	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 479](#)).
  2. Add the participating ports to this VLAN (see [“Configuring VLAN Interfaces” on page 481](#)), 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 ECS4510-28T 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  : ECS4100-26TX
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 ECS4100-26TX
Candidate      00-12-CF-0B-47-A0 ECS4100-26TX
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>ATC Trap Commands</i>		
<code>snmp-server enable port-traps atc broadcast-alarm-clear</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc broadcast-alarm-fire</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-apply</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-release</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-clear</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-fire</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-apply</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-release</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<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)

**Table 28: SNMP Commands** (Continued)

Command	Function	Mode
<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 \(165\)](#)

**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 \(164\)](#)

**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.

### Example

```
Console(config)#snmp-server enable traps authentication
Console(config)#
```

### Related Commands

[snmp-server host \(167\)](#)

**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 163](#)).
2. Create a view with the required notification messages ([page 175](#)).
3. Create a group that includes the required notify view ([page 172](#)).



4. Allow the switch to send SNMP traps; i.e., notifications ([page 166](#)).
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 163](#)).
  2. Create a remote SNMPv3 user to use in the message exchange process ([page 173](#)).
  3. Create a view with the required notification messages ([page 175](#)).
  4. Create a group that includes the required notify view ([page 172](#)).
  5. Allow the switch to send SNMP traps; i.e., notifications ([page 166](#)).
  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 \(166\)](#)

#### **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 mac-notification
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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 173).

### 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 \(167\)](#)

**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: public<sup>1</sup> (read only), private<sup>2</sup> (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 the 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 \(92\)](#)

**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 \(93\)](#)

**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: 50-500 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: 50-500 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 \(93\)](#)



# 6

## 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: 1-127 characters)

### Default Setting

1.3.6.1.4.1.259.10.1.46.104.1 - 1.3.6.1.4.1.259.10.1.46.102.26/

1.3.6.1.4.1.259.10.1.46.101.52

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 127](#)).

**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**

1.3.6.1.4.1.259.10.1.46.104.1 - 1.3.6.1.4.1.259.10.1.46.104.102.26/

1.3.6.1.4.1.259.10.1.46.101.52

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** 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
:

```



## 7

# 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, its associated timeout value will immediately begin to count down. Once the timeout value has reached zero seconds, the sFlow owner and its associated sampling sources will be deleted from the configuration.

### Example

This example shows an sflow collector being created on the switch.

```
Console(config)#sflow owner stat_server1 timeout 100 destination  
192.168.220.225 port 22500 max-datagram-size 512 version v5  
Console(config)#
```

This example shows how to modify the sFlow port number for an already configured collector.

```
Console(config)#sflow owner stat_server1 timeout 100 port 35100
Console(config)#
```

**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: 1-26/28/52)

*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(config)#interface ethernet 1/9
Console(config-if)#sflow polling-interval 10
Console(config-if)#
```

**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: 1-26/28/52)

*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: 1-26/28/52)

### 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 access<sup>3</sup> to the data ports.

**Table 35: Authentication Commands**

Command Group	Function
<a href="#">User Accounts and Privilege Levels</a>	Configures the basic user names and passwords for management access, and assigns a privilege level to specified command groups or individual commands
<a href="#">Authentication Sequence</a>	Defines logon authentication method and precedence
<a href="#">RADIUS Client</a>	Configures settings for authentication via a RADIUS server
<a href="#">TACACS+ Client</a>	Configures settings for authentication via a TACACS+ server
<a href="#">AAA</a>	Configures authentication, authorization, and accounting for network access
<a href="#">Web Server</a>	Enables management access via a web browser
<a href="#">Telnet Server</a>	Enables management access via Telnet
<a href="#">Secure Shell</a>	Provides secure replacement for Telnet
<a href="#">802.1X Port Authentication</a>	Configures host authentication on specific ports using 802.1X
<a href="#">Management IP Filter</a>	Configures IP addresses that are allowed management access
<a href="#">PPPoE Intermediate Agent</a>	Configures relay parameters required for sending authentication messages between a client and broadband remote access servers

3. For other methods of controlling client access, see [“General Security Measures” on page 267](#).

## 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 116), user authentication via a remote authentication server (page 201), and host access authentication for specific ports (page 245).

Table 36: User Access Commands

Command	Function	Mode
<a href="#">enable password</a>	Sets a password to control access to the Privileged Exec level	GC
<a href="#">username</a>	Establishes a user name-based authentication system at login	GC
<a href="#">privilege</a>	Assigns a privilege level to specified command groups or individual commands	GC
<a href="#">show privilege</a>	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 \(83\)](#)

[authentication enable \(206\)](#)

**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 74 and “Configuration Commands” on page 76.)

**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
<a href="#">authentication enable</a>	Defines the authentication method and precedence for command mode change	GC
<a href="#">authentication login</a>	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 (202)

**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 (203)

---

## 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
<a href="#">radius-server acct-port</a>	Sets the RADIUS server network port	GC
<a href="#">radius-server auth-port</a>	Sets the RADIUS server network port	GC
<a href="#">radius-server host</a>	Specifies the RADIUS server	GC
<a href="#">radius-server key</a>	Sets the RADIUS encryption key	GC
<a href="#">radius-server retransmit</a>	Sets the number of retries	GC
<a href="#">radius-server timeout</a>	Sets the interval between sending authentication requests	GC
<a href="#">show radius-server</a>	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 acct-port** This command sets the RADIUS server network port. 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 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*] [**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)

*key* - Encryption key used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes.  
(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. Use the **no** form to restore the default.

### Syntax

**radius-server key** *key-string*

**no radius-server key**

*key-string* - Encryption key 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 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
<a href="#">tacacs-server host</a>	Specifies the TACACS+ server and optional parameters	GC
<a href="#">tacacs-server key</a>	Sets the TACACS+ encryption key	GC
<a href="#">tacacs-server port</a>	Specifies the TACACS+ server network port	GC
<a href="#">tacacs-server retransmit</a>	Sets the number of retries	GC
<a href="#">tacacs-server timeout</a>	Sets the interval between sending authentication requests	GC
<a href="#">show tacacs-server</a>	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* [**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.

*key* - Encryption key used to authenticate logon access for the client.  
Enclose any string containing blank spaces in double quotes.  
(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 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 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
<a href="#">aaa accounting commands</a>	Enables accounting of Exec mode commands	GC
<a href="#">aaa accounting dot1x</a>	Enables accounting of 802.1X services	GC
<a href="#">aaa accounting exec</a>	Enables accounting of Exec services	GC
<a href="#">aaa accounting update</a>	Enables periodic updates to be sent to the accounting server	GC
<a href="#">aaa authorization commands</a>	Enables accounting of Exec mode commands	GC
<a href="#">aaa authorization exec</a>	Enables authorization of Exec sessions	GC
<a href="#">aaa group server</a>	Groups security servers in to defined lists	GC
<a href="#">server</a>	Configures the IP address of a server in a group list	SG
<a href="#">accounting dot1x</a>	Applies an accounting method to an interface for 802.1X service requests	IC
<a href="#">accounting commands</a>	Applies an accounting method to CLI commands entered by a user	Line
<a href="#">accounting exec</a>	Applies an accounting method to local console, Telnet or SSH connections	Line
<a href="#">authorization commands</a>	Applies an authorization method to CLI commands entered by a user	Line
<a href="#">authorization exec</a>	Applies an authorization method to local console, Telnet or SSH connections	Line
<a href="#">show accounting</a>	Displays all accounting information	PE
<a href="#">show authorization</a>	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

#### 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: 1-26/28/52)

### 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
<a href="#">ip http authentication</a>	Sets the method list for EXEC authorization of an EXEC session	GC
<a href="#">ip http port</a>	Specifies the port to be used by the web browser interface	GC
<a href="#">ip http server</a>	Allows the switch to be monitored or configured from a browser	GC
<a href="#">ip http secure-port</a>	Specifies the TCP port number for HTTPS	GC
<a href="#">ip http secure-server</a>	Enables HTTPS (HTTP/SSL) for encrypted communications	GC
<a href="#">show authorization</a>	Displays all authorization information	PE
<a href="#">show system</a>	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 \(220\)](#)

[ip http server \(230\)](#)

[show system \(98\)](#)

**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 \(230\)](#)  
[show system \(98\)](#)

**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 \(229\)](#)  
[show system \(98\)](#)

**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 \(231\)](#)  
[show system \(98\)](#)

**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 \(230\)](#)  
[copy tftp https-certificate \(105\)](#)  
[show system \(98\)](#)

---

## Telnet Server

This section describes commands used to configure Telnet management access to the switch.

**Table 44: Telnet Server Commands**

Command	Function	Mode
<a href="#">ip telnet max-sessions</a>	Specifies the maximum number of Telnet sessions that can simultaneously connect to this system	GC
<a href="#">ip telnet port</a>	Specifies the port to be used by the Telnet interface	GC
<a href="#">ip telnet server</a>	Allows the switch to be monitored or configured from Telnet	GC
<a href="#">telnet (client)</a>	Accesses a remote device using a Telnet connection	PE
<a href="#">show ip telnet</a>	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 \(243\)](#)

**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 \(241\)](#)

[show ssh \(244\)](#)

**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 \(118\)](#)

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

**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: 1-8 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 \(242\)](#)

[ip ssh save host-key \(242\)](#)

**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 \(241\)](#)

[ip ssh save host-key \(242\)](#)

[no ip ssh server \(238\)](#)

**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 dsa
Console#
```

## Related Commands

[ip ssh crypto host-key generate \(241\)](#)

**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
JlPdOkFgzLGMInvSNYQwiQXbKTBH0Z4mUZpE85PwxDZMacNBjBrRAAAAFQChb4vsdfQGNi jwvb
wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnr fwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOFT/yyEfbobMJZi8oGCst.SNOxrZZVnMqWrTYfdRkX7YKBw/Kjw6Bm
iFq70+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFACzWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAWecsigF/+DjKGWtPNIQgabKgYCw2
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>Supplicant Commands</i>		
<code>dot1x timeout auth-period</code>	Sets the time that a supplicant port waits for a response from the authenticator	IC
<code>dot1x timeout held-period</code>	Sets the time a port waits after the maximum start count has been exceeded before attempting to find another authenticator	IC
<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 \(251\)](#)

**dot1x timeout quiet-period** This command sets the time that a switch port waits after the maximum request count (see [page 248](#)) 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: 1-26/28/52)

### 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#
```

## Supplicant Commands

**dot1x timeout auth-period** This command sets the time that a supplicant port waits for a response from the authenticator. Use the **no** form to restore the default setting.

### Syntax

**dot1x timeout auth-period** *seconds*

**no dot1x timeout auth-period**

*seconds* - The number of seconds. (Range: 1-65535)

### Default

30 seconds

### Command Mode

Interface Configuration

### Command Usage

This command sets the time that the supplicant waits for a response from the authenticator for packets other than EAPOL-Start.

### Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout auth-period 60
Console(config-if)#
```

**dot1x timeout held-period** This command sets the time that a supplicant port waits before resending its credentials to find a new an authenticator. Use the **no** form to reset the default.

### Syntax

**dot1x timeout held-period** *seconds*

**no dot1x timeout held-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 held-period 120
Console(config-if)#
```

## 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: 1-26/28/52)

### 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 246](#)).
- ◆ *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 249](#)).
  - Control Mode – Dot1x port control mode ([page 250](#)).
  - 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 250](#)).
  - Reauth Period – Time after which a connected client must be re-authenticated ([page 251](#)).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client ([page 251](#)).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet ([page 252](#)).
  - 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 248](#)).

- 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 250).
  - Intrusion Action– Shows the port response to intrusion when authentication fails (page 247).
  - 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#
  
```

**PPPoE Intermediate Agent**

This section describes commands used to configure the PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

**Table 49: PPPoE Intermediate Agent Commands**

Command	Function	Mode
<code>pppoe intermediate-agent</code>	Enables the PPPoE IA globally on the switch	GC
<code>pppoe intermediate-agent format-type</code>	Sets the access node identifier, generic error message, or vendor identifier for the switch	GC
<code>pppoe intermediate-agent port-enable</code>	Enables the PPPoE IA on an interface	IC
<code>pppoe intermediate-agent port-format-type</code>	Sets the circuit-id, remote-id, or remote-id delimiter for an interface	IC
<code>pppoe intermediate-agent trust</code>	Sets the trust mode for an interface	IC
<code>pppoe intermediate-agent vendor-tag strip</code>	Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server	IC
<code>clear pppoe intermediate-agent statistics</code>	Clears PPPoE IA statistics	PE

Table 49: PPPoE Intermediate Agent Commands

Command	Function	Mode
<code>show pppoe intermediate-agent info</code>	Displays PPPoE IA configuration settings	PE
<code>show pppoe intermediate-agent statistics</code>	Displays PPPoE IA statistics	PE

**pppoe intermediate-agent** This command enables the PPPoE Intermediate Agent globally on the switch. Use the **no** form to disable this feature.

### Syntax

**[no] pppoe intermediate-agent**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ The switch inserts a tag identifying itself as a PPPoE Intermediate Agent residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports designated by the `pppoe intermediate-agent trust` command. The BRAS detects the presence of the subscriber's circuit-ID tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-ID attribute in PPP authentication and AAA accounting requests to a RADIUS server.
- ◆ PPPoE IA must be enabled globally by this command before this feature can be enabled on an interface using the `pppoe intermediate-agent port-enable` command.

### Example

```
Console(config)#pppoe intermediate-agent
Console(config)#
```

**pppoe intermediate-agent format-type** This command sets the access node identifier, generic error message, or vendor identifier for the switch. Use the **no** form to restore the default settings.

### Syntax

**pppoe intermediate-agent format-type** {**access-node-identifier** *node-id-string* | **generic-error-message** *error-message* | **vendor-id** *vendor-id-string*}

**no pppoe intermediate-agent format-type {access-node-identifier | generic-error-message}**

*node-id-string* - String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters)

*error-message* - An error message notifying the sender that the PPPoE Discovery packet was too large.

*vendor-id-string* - This tag is used to pass vendor proprietary information. The first four octets of the tag contain the vendor id and the remainder is unspecified. The high-order octet of the vendor id is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the Assigned Numbers RFC (RFC 1700). (Range: 0-4294967295)

**Default Setting**

- ◆ Access Node Identifier: IP address of the first IPv4 interface on the switch.
- ◆ Generic Error Message: PPPoE Discover packet too large to process. Try reducing the number of tags added.

**Command Mode**

Global Configuration

**Command Usage**

- ◆ The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets.
- ◆ These messages are forwarded to all trusted ports designated by the `pppoe intermediate-agent trust` command.

**Example**

```
Console(config)#pppoe intermediate-agent format-type access-node-identifier
billibong
Console(config)#
```

**pppoe intermediate-agent port-enable**

This command enables the PPPoE IA on an interface. Use the **no** form to disable this feature.

**Syntax**

**[no] pppoe intermediate-agent port-enable**

**Default Setting**

Disabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

PPPoE IA must also be enabled globally on the switch for this command to take effect.

### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-enable
Console(config-if)#
```

### pppoe intermediate-agent port-format-type

This command sets the circuit-id, remote-id, or remote-id delimiter for an interface. Use the **no** form to restore the default settings.

#### Syntax

**pppoe intermediate-agent port-format-type** {**circuit-id** *circuit-id-string* | **remote-id** *remote-id-string* | **remote-id-delimiter** {**enable** | *ascii-code*}}

**no pppoe intermediate-agent port-format-type** {**circuit-id** | **remote-id** | **remote-id-delimiter enable**}

*circuit-id-string* - String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters)

*remote-id-string* - String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters)

**remote-id-delimiter enable** - Enables a user-specified delimiter value for the remote ID.

*ascii-code* - A character used to separate components in the remote circuit ID value. (Range: 0-255)

#### Default Setting

circuit-id: unit/port:vlan-id or 0/trunk-id:vlan-id

remote-id: port MAC address

remote-id-delimiter: ASCII code 35, ASCII character "#"

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ The PPPoE server extracts the Line-ID tag from PPPoE discovery stage messages, and uses the Circuit-ID field of that tag as a NAS-Port-ID attribute in AAA access and accounting requests.
- ◆ The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then

forwards these packets to the PPPoE server. The tag contains the Line-ID of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.

- ◆ Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-Id tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients using the `pppoe intermediate-agent vendor-tag strip` command.
- ◆ If the remote-id is unspecified, the port name will be used for this parameter. If the port name is not configured, the remote-id is set to the port MAC (yy-yy-yy-yy-yy-yy#), where # is the default delimiter.

### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id
ECS4100-26TX
Console(config-if)#
```

**pppoe intermediate-agent trust** This command sets an interface to trusted mode to indicate that it is connected to a PPPoE server. Use the **no** form to set an interface to untrusted mode.

### Syntax

**[no] pppoe intermediate-agent trust**

### Default Setting

Untrusted

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.
- ◆ At least one trusted interface must be configured on the switch for the PPPoE IA to function.

### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent trust
Console(config-if)#
```

**pppoe intermediate-agent vendor-tag strip** This command enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. Use the **no** form to disable this feature.

#### Syntax

**[no] pppoe intermediate-agent vendor-tag strip**

#### Default Setting

Disabled

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

This command only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

#### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent vendor-tag strip
Console(config-if)#
```

**clear pppoe intermediate-agent statistics** This command clears statistical counters for the PPPoE Intermediate Agent.

#### Syntax

**clear pppoe intermediate-agent statistics interface** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Stack unit (Range: 1)

*port* - Port number (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-26)

#### Command Mode

Privileged Exec

#### Example

```
Console#clear pppoe intermediate-agent statistics
Console#
```



**show pppoe intermediate-agent info** This command displays configuration settings for the PPPoE Intermediate Agent.  
**Syntax**

```
show pppoe intermediate-agent info [interface [interface]]  

interface  

ethernet unit/port  

unit - Stack unit. (Range: 1)  

port - Port number (Range: 1-26/28/52)  

port-channel channel-id (Range: 1-26)
```

**Command Mode**  
 Privileged Exec

**Example**

```
Console#show pppoe intermediate-agent info
PPPoE Intermediate Agent Global Status           : Enabled
PPPoE Intermediate Agent Admin Access Node Identifier : 192.168.0.2
PPPoE Intermediate Agent Oper Access Node Identifier : 192.168.0.2
PPPoE Intermediate Agent Admin Generic Error Message :
  PPPoE Discover packet too large to process. Try reducing the number of tags
  added.
PPPoE Intermediate Agent Oper Generic Error Message :
  PPPoE Discover packet too large to process. Try reducing the number of tags
  added.
Console#show pppoe intermediate-agent info interface ethernet 1/1
Interface PPPoE IA Trusted Vendor-Tag Strip Admin Circuit-ID Admin Remote-ID
-----
Eth 1/2   Yes      No       Yes                ECS4600-26TX      ECS4600-26TX
                                                Oper Circuit-ID  Oper Remote-ID
-----
                                                1/1:vid         70-72-CF-7C-F3-A4
Console#
```

**show pppoe intermediate-agent statistics** This command displays statistics for the PPPoE Intermediate Agent.  
**Syntax**

```
show pppoe intermediate-agent statistics interface [interface]  

interface  

ethernet unit/port  

unit - Unit identifier. (Range: 1)  

port - Port number. (Range: 1-26/28/52)  

port-channel channel-id (Range: 1-26)
```

**Command Mode**  
 Privileged Exec

**Example**

```

Console#show pppoe intermediate-agent statistics interface ethernet 1/1
Eth 1/1 statistics
-----
Received :      All      PADI      PADO      PADR      PADS      PADT
             -----
                   3          0          0          0          0          3

Dropped  : Response from untrusted  Request towards untrusted  Malformed
             -----
                   0                          0          0

Console#
  
```

**Table 50: show pppoe intermediate-agent statistics - display description**

Field	Description
<i>Received</i>	
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-Confirmation
PADT	PPPoE Active Discovery Terminate
<i>Dropped</i>	
Response from untrusted	Response from an interface which not been configured as trusted.
Request towards untrusted	Request sent to an interface which not been configured as trusted.
Malformed	Corrupted PPPoE message.

# 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 51: 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
DHCPv6 Snooping*	Filters untrusted DHCPv6 messages on unsecure ports by building and maintaining a DHCPv6 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
IPv6 Source Guard*	Filters IPv6 traffic on insecure ports for which the source address cannot be identified via DHCPv6 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 52: 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 \(387\)](#)

**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 of 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 \(387\)](#)

[shutdown \(378\)](#)

[mac-address-table static \(436\)](#)

**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: 1-26/28/52)

### 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 53: 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"> <li>◆ Secure/Down – Port security is disabled.</li> <li>◆ Secure/Up – Port security is enabled.</li> <li>◆ Shutdown – Port is shut down due to a response to a port security violation.</li> </ul>
Intrusion Action	The configured intrusion response.

**Table 53: 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 54: 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 249](#)).
- ◆ 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 port-mac-filter` command.
- ◆ Up to 64 filter tables can be defined.
- ◆ There is no limitation on the number of entries that can be 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 dynamic-qos** Use this command to enable the dynamic QoS feature for an authenticated port. 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 55: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	<b>service-policy-in</b> = <i>policy-map-name</i>	service-policy-in=p1
Rate Limit	<b>rate-limit-input</b> = <i>rate (Kbps)</i>	rate-limit-input=100 (Kbps)
	<b>rate-limit-output</b> = <i>rate (Kbps)</i>	rate-limit-output=200 (Kbps)
802.1p	<b>switchport-priority-default</b> = <i>value</i>	switchport-priority-default=2
IP ACL	<b>ip-access-group-in</b> = <i>ip-acl-name</i>	ip-access-group-in=ip4acl
IPv6 ACL	<b>ipv6-access-group-in</b> = <i>ipv6-acl-name</i>	ipv6-access-group-in=ipv6acl
MAC ACL	<b>mac-access-group-in</b> = <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. GVRP is not used to create the VLANs.
- ◆ 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: 1-26/28/52)

### 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: 1-26/28/52)

### 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
Link Detection                  : Disabled
Detection Mode                  : Link-down
Detection Action                : Trap
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: 1-26/28/52)

**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 188](#)).

**Note:** Web authentication cannot be configured on trunk ports.

**Table 56: 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: 1-26/28/52)

### 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: 1-26/28/52)

*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: 1-26/28/52)

### 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 57: DHCP Snooping Commands**

Command	Function	Mode
<code>ip dhcp snooping</code>	Enables DHCP snooping globally	GC
<code>ip dhcp snooping information option</code>	Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id	GC
<code>ip dhcp snooping information option encode no-subtype</code>	Disables use of sub-type and sub-length for the CID/RID in Option 82 information	GC
<code>ip dhcp snooping information option remote-id</code>	Sets the remote ID to the switch's IP address, MAC address, arbitrary string, TR-101 compliant node identifier, or removes VLAN ID from the end of the TR101 field	GC
<code>ip dhcp snooping information option tr101 board-id</code>	Sets the board identifier used in Option 82 information based on TR-101 syntax	GC
<code>ip dhcp snooping information policy</code>	Sets the information option policy for DHCP client packets that include Option 82 information	GC
<code>ip dhcp snooping verify mac-address</code>	Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC
<code>ip dhcp snooping vlan</code>	Enables DHCP snooping on the specified VLAN	GC
<code>ip dhcp snooping information option circuit-id</code>	Enables or disables the use of DHCP Option 82 information circuit-id suboption	IC

Table 57: 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>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 is 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 \(299\)](#)

[ip dhcp snooping trust \(302\)](#)

### 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, the no form with the encode no-subtype keyword to enable use of sub-type and sub-length in CID/RID fields, or the **no** form with the **remote-id** keyword to set the remote ID to the switch's MAC address encoded in hexadecimal.

### Syntax

#### ip dhcp snooping information option

[**encode no-subtype**] [**remote-id** {**ip-address** [**encode** {**ascii** | **hex**}}] | [**mac-address** [**encode** {**ascii** | **hex**}}] | **string** *string*}]

#### no ip dhcp snooping information option [**encode no-subtype**]

[**remote-id** [**ip-address encode**] | [**mac-address encode**]]

**encode no-subtype** - Disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.

**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)

### Default Setting

Option 82: Disabled

CID/RID sub-type: Enabled

Remote ID: MAC address (hexadecimal)

### 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 58: 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, 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

MAC address: hexadecimal  
tr101 no-vlan-field: disabled

### 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.

#### 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 \(291\)](#)

[ip dhcp snooping vlan \(299\)](#)

[ip dhcp snooping trust \(302\)](#)

**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 \(291\)](#)

[ip dhcp snooping trust \(302\)](#)

**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 59: 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 \(291\)](#)

[ip dhcp snooping vlan \(299\)](#)

**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-Num	Circuit-ID mode	Circuit-ID Value	Circuit-ID TR101 VLAN	Carry To Client
Eth 1/1	No	16	VLAN-Unit-Port	---	enabled	disabled
Eth 1/2	No	16	VLAN-Unit-Port	---	enabled	disabled
Eth 1/3	No	16	VLAN-Unit-Port	---	enabled	disabled
Eth 1/4	No	16	VLAN-Unit-Port	---	enabled	disabled
Eth 1/5	No	16	VLAN-Unit-Port	---	enabled	disabled
.						
.						
.						

**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#
```



## DHCPv6 Snooping

DHCPv6 snooping allows a switch to protect a network from rogue DHCPv6 servers or other devices which send port-related information to a DHCPv6 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv6 snooping.

**Table 60: DHCP Snooping Commands**

Command	Function	Mode
<code>ipv6 dhcp snooping</code>	Enables DHCPv6 snooping globally	GC
<code>ipv6 dhcp snooping option remote-id</code>	Enables insertion of DHCPv6 Option 37 relay agent remote-id	GC
<code>ipv6 dhcp snooping option remote-id policy</code>	Sets the information option policy for DHCPv6 client packets that include Option 37 information	GC
<code>ipv6 dhcp snooping vlan</code>	Enables DHCPv6 snooping on the specified VLAN	GC
<code>ipv6 dhcp snooping max-binding</code>	Sets the maximum number of entries which can be stored in the binding database for an interface	IC
<code>ipv6 dhcp snooping trust</code>	Configures the specified interface as trusted	IC
<code>clear ipv6 dhcp snooping binding</code>	Clears DHCPv6 snooping binding table entries from RAM	PE
<code>clear ipv6 dhcp snooping statistics</code>	Clears statistical counters for DHCPv6 snooping client, server and relay packets	PE
<code>show ipv6 dhcp snooping</code>	Shows the DHCPv6 snooping configuration settings	PE
<code>show ipv6 dhcp snooping binding</code>	Shows the DHCPv6 snooping binding table entries	PE
<code>show ipv6 dhcp snooping statistics</code>	Shows statistics for DHCPv6 snooping client, server and relay packets	PE

**ipv6 dhcp snooping** This command enables DHCPv6 snooping globally. Use the **no** form to restore the default setting.

### Syntax

**[no] ipv6 dhcp snooping**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ Network traffic may be disrupted when malicious DHCPv6 messages are received from an outside source. DHCPv6 snooping is used to filter DHCPv6 messages received on an unsecure interface from outside the network or fire

wall. When DHCPv6 snooping is enabled globally by this command, and enabled on a VLAN interface by the `ipv6 dhcp snooping vlan` command, DHCP messages received on an untrusted interface (as specified by the `no ipv6 dhcp snooping trust` command) from a device not listed in the DHCPv6 snooping table will be dropped.

- ◆ When enabled, DHCPv6 messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCPv6 snooping.
- ◆ Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IPv6 address, lease time, binding type, VLAN identifier, and port identifier.
- ◆ When DHCPv6 snooping is enabled, the rate limit for the number of DHCPv6 messages that can be processed by the switch is 100 packets per second. Any DHCPv6 packets in excess of this limit are dropped.
- ◆ Filtering rules are implemented as follows:
  - If global DHCPv6 snooping is disabled, all DHCPv6 packets are forwarded.
  - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCPv6 packet is received, DHCPv6 packets are forwarded for a *trusted* port as described below.
  - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, DHCP packets are processed according to message type as follows:

#### *DHCP Client Packet*

- Request: Update entry in binding cache, recording client's DHCPv6 Unique Identifier (DUID), server's DUID, Identity Association (IA) type, IA Identifier, and address (4 message exchanges to get IPv6 address), and forward to trusted port.
- Solicit: Add new entry in binding cache, recording client's DUID, IA type, IA ID (2 message exchanges to get IPv6 address with rapid commit option, otherwise 4 message exchanges), and forward to trusted port.
- Decline: If no matching entry is found in binding cache, drop this packet.
- Renew, Rebind, Release, Confirm: If no matching entry is found in binding cache, drop this packet.
- If the DHCPv6 packet is not a recognizable type, it is dropped.

If a DHCPv6 packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

### *DHCP Server Packet*

- If a DHCP server packet is received on an *untrusted* port, drop this packet and add a log entry in the system.
  - If a DHCPv6 Reply packet is received from a server on a *trusted* port, it will be processed in the following manner:
    - a. Check if IPv6 address in IA option is found in binding table:
      - If yes, continue to C.
      - If not, continue to B.
    - b. Check if IPv6 address in IA option is found in binding cache:
      - If yes, continue to C.
      - If not, check failed, and forward packet to trusted port.
    - c. Check status code in IA option:
      - If successful, and entry is in binding table, update lease time and forward to original destination.
      - If successful, and entry is in binding cache, move entry from binding cache to binding table, update lease time and forward to original destination.
      - Otherwise, remove binding entry. and check failed.
      - If a DHCPv6 Relay packet is received, check the relay message option in Relay-Forward or Relay-Reply packet, and process client and server packets as described above.
- 
- ◆ If DHCPv6 snooping is globally disabled, all dynamic bindings are removed from the binding table.
  - ◆ *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which the switch submits a client request to the DHCPv6 server must be configured as trusted (using the `ipv6 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 DHCPv6 server. Also, when the switch sends out DHCPv6 client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCPv6 server, any packets received from untrusted ports are dropped.

### Example

This example enables DHCPv6 snooping globally for the switch.

```
Console(config)#ipv6 dhcp snooping
Console(config)#
```

### Related Commands

[ipv6 dhcp snooping vlan \(310\)](#)

[ipv6 dhcp snooping trust \(311\)](#)

### ipv6 dhcp snooping option remote-id

This command enables the insertion of remote-id option 37 information into DHCPv6 client messages. Remote-id option information such as the port attached to the client, DUID, and VLAN ID is used by the DHCPv6 server to assign preassigned configuration data specific to the DHCPv6 client. Use the **no** form of the command to disable this function.

### Syntax

**[no] ipv6 dhcp snooping option remote-id**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ DHCPv6 provides a relay mechanism for sending information about the switch and its DHCPv6 clients to the DHCPv6 server. Known as DHCPv6 Option 37, it allows compatible DHCPv6 servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- ◆ When DHCPv6 Snooping Information Option 37 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCPv6 request packets forwarded by the switch and in reply packets sent back from the DHCPv6 server.
- ◆ When the DHCPv6 Snooping Option 37 is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCPv6 client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- ◆ DHCPv6 snooping must be enabled for the DHCPv6 Option 37 information to be inserted into packets. When enabled, the switch will either drop, keep or

remove option 37 information in incoming DHCPv6 packets. Packets are processed as follows:

- If an incoming packet is a DHCPv6 request packet with option 37 information, it will modify the option 37 information according to settings specified with `ipv6 dhcp snooping option remote-id policy` command.
  - If an incoming packet is a DHCPv6 request packet without option 37 information, enabling the DHCPv6 snooping information option will add option 37 information to the packet.
  - If an incoming packet is a DHCPv6 reply packet with option 37 information, enabling the DHCPv6 snooping information option will remove option 37 information from the packet.
- ◆ When this switch inserts Option 37 information in DHCPv6 client request packets, the switch's MAC address (hexadecimal) is used for the remote ID.

### Example

This example enables the DHCPv6 Snooping Remote-ID Option.

```
Console(config)#ipv6 dhcp snooping option remote-id
Console(config)#
```

### ipv6 dhcp snooping option remote-id policy

This command sets the remote-id option policy for DHCPv6 client packets that include Option 37 information. Use the **no** form to disable this function.

#### Syntax

**ipv6 dhcp snooping option remote-id policy {drop | keep | replace}**

**no ipv6 dhcp snooping option remote-id policy**

**drop** - Drops the client's request packet instead of relaying it.

**keep** - Retains the Option 37 information in the client request, and forwards the packets to trusted ports.

**replace** - Replaces the Option 37 remote-ID in the client's request with the relay agent's remote-ID (when DHCPv6 snooping is enabled), and forwards the packets to trusted ports.

#### Default Setting

drop

#### Command Mode

Global Configuration

#### Command Usage

When the switch receives DHCPv6 packets from clients that already include DHCP Option 37 information, the switch can be configured to set the action policy for

these packets. The switch can either drop the DHCPv6 packets, keep the existing information, or replace it with the switch's relay agent information.

### Example

This example configures the switch to keep existing remote-id option 37 information within DHCPv6 client packets and forward it.

```
Console(config)#ipv6 dhcp snooping option remote-id policy keep
Console(config)#
```

**ipv6 dhcp snooping vlan** This command enables DHCPv6 snooping on the specified VLAN. Use the **no** form to restore the default setting.

### Syntax

**[no] ipv6 dhcp snooping vlan** {*vlan-id* | *vlan-range*}

*vlan-id* - ID of a configured VLAN (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

### Command Mode

Global Configuration

### Command Usage

- ◆ When DHCPv6 snooping enabled globally using the [ipv6 dhcp snooping](#) command, and enabled on a VLAN with this command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN as specified by the [ipv6 dhcp snooping trust](#) command.
- ◆ When the DHCPv6 snooping is globally disabled, DHCPv6 snooping can still be configured for specific VLANs, but the changes will not take effect until DHCPv6 snooping is globally re-enabled.
- ◆ When DHCPv6 snooping is enabled globally, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

### Example

This example enables DHCPv6 snooping for VLAN 1.

```
Console(config)#ipv6 dhcp snooping vlan 1
Console(config)#
```

### Related Commands

[ipv6 dhcp snooping \(305\)](#)

[ipv6 dhcp snooping trust \(311\)](#)

**ipv6 dhcp snooping max-binding** This command sets the maximum number of entries which can be stored in the binding database for an interface. Use the **no** form to restore the default setting.

### Syntax

**ipv6 dhcp snooping max-binding** *count*

**no ipv6 dhcp snooping max-binding**

*count* - Maximum number of entries. (Range: 1-5)

### Default Setting

5

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Example

This example sets the maximum number of binding entries to 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 dhcp snooping max-binding 1
Console(config-if)#
```

**ipv6 dhcp snooping trust** This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

### Syntax

**[no] ipv6 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 DHCPv6 servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.

- ◆ When DHCPv6 snooping is enabled globally using the `ipv6 dhcp snooping` command, and enabled on a VLAN with `ipv6 dhcp snooping vlan` command, DHCPv6 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 ipv6 dhcp snooping trust` command.
- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCPv6 snooping bindings associated with this port are removed.
- ◆ *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which it submits a client request to the DHCPv6 server must be configured as trusted.

### Example

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ipv6 dhcp snooping trust
Console(config-if)#
```

### Related Commands

[ipv6 dhcp snooping \(305\)](#)

[ipv6 dhcp snooping vlan \(310\)](#)

### clear ipv6 dhcp snooping binding

This command clears DHCPv6 snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

### Syntax

**clear ipv6 dhcp snooping binding** [*mac-address ipv6-address*]

*mac-address* - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

*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.

### Command Mode

Privileged Exec

### Example

```
Console(config)#clear ipv6 dhcp snooping binding 00-12-cf-01-02-03 2001::1
Console(config)#
```



**clear ipv6 dhcp snooping statistics** This command clears statistical counters for DHCPv6 snooping client, server and relay packets.

**Command Mode**  
Privileged Exec

**Example**

```
Console(config)#clear ipv6 dhcp snooping statistics
Console(config)#
```

**show ipv6 dhcp snooping** This command shows the DHCPv6 snooping configuration settings.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ipv6 dhcp snooping
Global DHCPv6 Snooping status: disabled
DHCPv6 Snooping remote-id option status: enabled
DHCPv6 Snooping remote-id policy: drop
DHCPv6 Snooping is configured on the following VLANs:
  1,
Interface          Trusted          Max-binding    Current-binding
-----
Eth 1/1             No               5              0
Eth 1/2             No               5              0
Eth 1/3             No               5              0
Eth 1/4             No               5              0
Eth 1/5             Yes              5              0
.
.
```

**show ipv6 dhcp snooping binding** This command shows the DHCPv6 snooping binding table entries.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ipv6 dhcp snooping binding
NA - Non-temporary address
TA - Temporary address
-----
Link-layer Address: 00-13-49-aa-39-26
IPv6 Address                               Lifetime  VLAN Port  Type
-----
2001:b021:1435:5612:ab3c:6792:a452:6712   2591998  1  Eth 1/5  NA
-----
Link-layer Address: 00-12-cf-01-02-03
```

```

IPv6 Address                               Lifetime  VLAN Port  Type
-----
2001:b000::1    2591912    1 Eth 1/3  NA
Console#

```

**show ipv6 dhcp snooping statistics** This command shows statistics for DHCPv6 snooping client, server and relay packets.

**Command Mode**  
Privileged Exec

### Example

```

Console#show ipv6 dhcp snooping statistics
DHCPv6 Snooping Statistics:
  Client Packet: Solicit, Request, Confirm, Renew, Rebind,
                  Decline, Release, Information-request
  Server Packet: Advertise, Reply, Reconfigure
  Relay Packet:  Relay-forward, Relay-reply
State   Client   Server   Relay   Total
-----
Received 10       9        0       19
Sent     9        9        0       18
Dropped  1        0        0        1
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 290](#)). 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 61: IPv4 Source Guard Commands**

Command	Function	Mode
<code>ip source-guard binding</code>	Adds a static address to the source-guard binding table	GC
<code>ip source-guard</code>	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC
<code>ip source-guard max-binding</code>	Sets the maximum number of entries that can be bound to an interface	IC
<code>ip source-guard mode</code>	Sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table	IC
<code>clear ip source-guard binding blocked</code>	Remove all blocked records	PE

Table 61: IPv4 Source Guard Commands (Continued)

Command	Function	Mode
<code>show ip source-guard</code>	Shows whether source guard is enabled or disabled on each interface	PE
<code>show ip source-guard binding</code>	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: 1-26/28/52)

### 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 320).

- ◆ 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 \(317\)](#)

[ip dhcp snooping \(291\)](#)

[ip dhcp snooping vlan \(299\)](#)

**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 291](#)), 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 \(315\)](#)

[ip dhcp snooping \(291\)](#)

[ip dhcp snooping vlan \(299\)](#)

**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  MAC Table
-----  -
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 290](#))

**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: 1-26/28/52)

#### 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#

```

## IPv6 Source Guard

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled (see [“DHCPv6 Snooping” on page 305](#)). IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes commands used to configure IPv6 Source Guard.

**Table 62: IPv6 Source Guard Commands**

Command	Function	Mode
<code>ipv6 source-guard binding</code>	Adds a static address to the source-guard binding table	GC
<code>ipv6 source-guard</code>	Configures the switch to filter inbound traffic based on source IP address	IC
<code>ipv6 source-guard max-binding</code>	Sets the maximum number of entries that can be bound to an interface	IC
<code>show ipv6 source-guard</code>	Shows whether source guard is enabled or disabled on each interface	PE
<code>show ipv6 source-guard binding</code>	Shows the source guard binding table	PE

**ipv6 source-guard binding** This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

### Syntax

**ipv6 source-guard binding** *mac-address* **vlan** *vlan-id* *ipv6-address*  
**interface** *interface*

**no ipv6 source-guard binding** *mac-address* **vlan** *vlan-id*

*mac-address* - A valid unicast MAC address.

*vlan-id* - ID of a configured VLAN (Range: 1-4094)

*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.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

### Default Setting

No configured entries

### Command Mode

Global Configuration

### Command Usage

- ◆ Table entries include an associated MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Snooping, Dynamic-DHCPv6-Snooping), VLAN identifier, and port identifier.
- ◆ Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.
- ◆ All static entries are configured with an infinite lease time, which is indicated with a value of zero by the `show ipv6 source-guard` command.
- ◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 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:
  - If there is no entry with same and MAC address and IPv6 address, a new entry is added to binding table using static IPv6 source guard binding.
  - If there is an entry with same MAC address and IPv6 address, and the type of entry is static IPv6 source guard binding, then the new entry will replace the old one.
  - If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IPv6 source guard binding.
  - Only unicast addresses are accepted for static bindings.

### Example

This example configures a static source-guard binding on port 5.

```
Console(config)#ipv6 source-guard binding 00-ab-11-cd-23-45 vlan 1 2001::1
interface ethernet 1/5
Console(config)#
```

### Related Commands

[ipv6 source-guard \(324\)](#)

[ipv6 dhcp snooping \(305\)](#)  
[ipv6 dhcp snooping vlan \(310\)](#)

**ipv6 source-guard** This command configures the switch to filter inbound traffic based on the source IP address stored in the binding table. Use the **no** form to disable this function.

#### Syntax

**ipv6 source-guard sip**  
**no ipv6 source-guard**

#### 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.
- ◆ This command checks the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table. Use the **no ipv6 source guard** command to disable this function on the selected port.
- ◆ After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.
- ◆ Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Snooping, Dynamic-DHCPv6-Snooping), VLAN identifier, and port identifier.
- ◆ Static addresses entered in the source guard binding table with the [ipv6 source-guard binding](#) command are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.
- ◆ If IPv6 source guard is enabled, an inbound packet's source IPv6 address 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 ND snooping and DHCPv6 snooping are disabled, IPv6 source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, the packet will be forwarded.
  - If ND snooping or DHCPv6 snooping is enabled, IPv6 source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.
  - If IPv6 source guard is enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCPv6 snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets allowed by DHCPv6 snooping.
  - Only IPv6 global 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)#ipv6 source-guard sip
Console(config-if)#
```

### Related Commands

[ipv6 source-guard binding \(322\)](#)

[ipv6 dhcp snooping \(305\)](#)

[ipv6 dhcp snooping vlan \(310\)](#)

**ipv6 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

**ipv6 source-guard max-binding** *number*

**no ipv6 source-guard max-binding**

*number* - The maximum number of IPv6 addresses that can be mapped to an interface in the binding table. (Range: 1-5)

### Default Setting

5

### 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, including both dynamic entries discovered by ND snooping, DHCPv6 snooping, and static entries set by the `ipv6 source-guard` command.
- ◆ IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.
- ◆ If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by the **ipv6 source-guard max-binding** command. In other words, no new entries will be added to the IPv6 source guard binding table.
- ◆ If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

### Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard max-binding 1
Console(config-if)#
```

**show ipv6 source-guard** This command shows whether IPv6 source guard is enabled or disabled on each interface, and the maximum allowed bindings.

### Command Mode

Privileged Exec

### Example

```
Console#show ipv6 source-guard
Interface  Filter-type  Max-binding
-----
Eth 1/1    DISABLED      5
Eth 1/2    DISABLED      5
Eth 1/3    DISABLED      5
Eth 1/4    DISABLED      5
Eth 1/5    SIP           1
Eth 1/6    DISABLED      5
```

:

**show ipv6 source-guard binding** This command shows the IPv6 source guard binding table.

#### Syntax

**show ipv6 source-guard binding [dynamic | static]**

**dynamic** - Shows dynamic entries configured with ND Snooping or DHCPv6 Snooping commands (see [page 305](#))

**static** - Shows static entries configured with the [ipv6 source-guard binding](#) command.

#### Command Mode

Privileged Exec

#### Example

```

Console#show ipv6 source-guard binding
MAC Address      IPv6 Address          VLAN Interface Type
-----
00AB-11CD-2345   2001::1              1  Eth 1/5  STA
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 63: ARP Inspection Commands**

Command	Function	Mode
<a href="#">ip arp inspection</a>	Enables ARP Inspection globally on the switch	GC
<a href="#">ip arp inspection filter</a>	Specifies an ARP ACL to apply to one or more VLANs	GC
<a href="#">ip arp inspection log-buffer logs</a>	Sets the maximum number of entries saved in a log message, and the rate at these messages are sent	GC

Table 63: ARP Inspection Commands (Continued)

Command	Function	Mode
<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.

### 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 366](#).
- ◆ 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 (Port, Static Aggregation)

### 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 (Port, Static Aggregation)

### 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: 1-26/28/52)

### 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

### Command Usage

Enter this command to display the configuration settings for all VLANs, or display the settings for a specific VLAN by entering the VLAN identifier.

### 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 64: DoS Protection Commands**

Command	Function	Mode
<a href="#">dos-protection echo-charge</a>	Protects against DoS echo/charge attacks	GC
<a href="#">dos-protection smurf</a>	Protects against DoS smurf attacks	GC
<a href="#">dos-protection tcp-flooding</a>	Protects against DoS TCP-flooding attacks	GC
<a href="#">dos-protection tcp-null-scan</a>	Protects against DoS TCP-null-scan attacks	GC
<a href="#">dos-protection tcp-syn-fin-scan</a>	Protects against DoS TCP-SYN/FIN-scan attacks	GC
<a href="#">dos-protection tcp-xmas-scan</a>	Protects against DoS TCP-XMAS-scan attacks	GC
<a href="#">dos-protection udp-flooding</a>	Protects against DoS UDP-flooding attacks	GC
<a href="#">dos-protection win-nuke</a>	Protects against DoS WinNuke attacks	GC
<a href="#">show dos-protection</a>	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

**dos-protection echo-charge** [**bit-rate-in-kilo** *rate*]

**no dos-protection echo-charge** [**bit-rate-in-kilo**]

*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

**dos-protection tcp-flooding [bit-rate-in-kilo rate]**

**no dos-protection tcp-flooding [bit-rate-in-kilo]**

*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

**dos-protection udp-flooding [bit-rate-in-kilo *rate*]**

**no dos-protection udp-flooding [bit-rate-in-kilo]**

*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-nuke** 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

**dos-protection win-nuke [bit-rate-in-kilo *rate*]**

**no dos-protection win-nuke [bit-rate-in-kilo]**

*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-nuke bit-rate-in-kilo 65
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 65: Commands for Configuring Traffic Segmentation**

Command	Function	Mode
<a href="#">traffic-segmentation</a>	Enables traffic segmentation	GC
<a href="#">traffic-segmentation session</a>	Creates a client session	GC
<a href="#">traffic-segmentation uplink/ downlink</a>	Configures uplink/downlink ports for client sessions	GC
<a href="#">traffic-segmentation uplink-to-uplink</a>	Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions	GC
<a href="#">show traffic-segmentation</a>	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 66: Traffic Segmentation Forwarding**

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
<b>Session #1 Downlink Ports</b>	Blocking	Forwarding	Blocking	Blocking	Blocking
<b>Session #1 Uplink Ports</b>	Forwarding	Forwarding	Blocking	Blocking/Forwarding*	Forwarding
<b>Session #2 Downlink Ports</b>	Blocking	Blocking	Blocking	Forwarding	Blocking
<b>Session #2 Uplink Ports</b>	Blocking	Blocking/Forwarding*	Forwarding	Forwarding	Forwarding
<b>Normal Ports</b>	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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-26)

### 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
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 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 67: Access Control List Commands**

Command Group	Function
IPv4 ACLs	Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code
IPv6 ACLs	Configures ACLs based on IPv6 addresses, DSCP traffic class, or next header type
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type
ARP ACLs	Configures ACLs based on ARP messages addresses
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port

## IPv4 ACLs

The commands in this section configure 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 68: 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 1K rules.

### Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

### Related Commands

[permit, deny \(348\)](#)

[show ip access-list \(353\)](#)

**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 \(348\)](#)

[Time Range \(151\)](#)

**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* – Protocol<sup>4</sup> source port number. (Range: 0-65535)

*dport* – Protocol<sup>4</sup> 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 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 \(348\)](#)

[Time Range \(151\)](#)

**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.

### 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)#int eth 1/2  
Console(config-if)#ip access-group david in  
Console(config-if)#
```

### Related Commands

[show ip access-list \(353\)](#)

[Time Range \(151\)](#)



**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 \(348\)](#)

## IPv6 ACLs

The commands in this section configure 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 69: 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 \(Standard IPv6 ACL\) \(355\)](#)

[permit, deny \(Extended IPv6 ACL\) \(356\)](#)

[ipv6 access-group \(359\)](#)

[show ipv6 access-list \(360\)](#)

**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 \(354\)](#)

[Time Range \(151\)](#)

**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}
  [dscp dscp] [next-header next-header]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
  [time-range time-range-name]
```

```
no {permit | deny}
  {any | host source-ipv6-address | source-ipv6-address/prefix-length}
  {any | destination-ipv6-address/prefix-length}
  [dscp dscp] [next-header next-header]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
```

**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* - Protocol<sup>5</sup> source port number. (Range: 0-65535)

*dport* - Protocol<sup>4</sup> 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 ip 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 \(354\)](#)

[Time Range \(151\)](#)

**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.

### 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 \(360\)](#)

[Time Range \(151\)](#)

**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 \(359\)](#)

**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 \(Standard IPv6 ACL\) \(355\)](#)

[permit, deny \(Extended IPv6 ACL\) \(356\)](#)

[ipv6 access-group \(359\)](#)

## MAC ACLs

The commands in this section configure 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 70: MAC ACL Commands**

Command	Function	Mode
<a href="#">access-list mac</a>	Creates a MAC ACL and enters configuration mode	GC
<a href="#">permit, deny</a>	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
<a href="#">mac access-group</a>	Binds a MAC ACL to a port	IC
<a href="#">show mac access-group</a>	Shows port assignments for MAC ACLs	PE
<a href="#">show mac access-list</a>	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 2048 rules.

### Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

### Related Commands

[permit, deny \(361\)](#)

[mac access-group \(364\)](#)

[show mac access-list \(365\)](#)

**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*<sup>6</sup> – 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*<sup>6</sup> – Class-of-Service bitmask. (Range: 0-7)

*vid* – VLAN ID. (Range: 1-4094)

*vid-bitmask*<sup>6</sup> – VLAN bitmask. (Range: 1-4095)

*ethertype* – A specific Ethernet protocol number. (Range: 0-ffff hex)

*ethertype-bitmask*<sup>6</sup> – 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.
- ◆ 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.

---

6. For all bitmasks, “1” means relevant and “0” means ignore.

### 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 \(361\)](#)

[Time Range \(151\)](#)

**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.

### 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 \(365\)](#)

[Time Range \(151\)](#)

**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 \(364\)](#)

**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 \(361\)](#)

[mac access-group \(364\)](#)

## ARP ACLs

The commands in this section configure 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 71: ARP ACL Commands

Command	Function	Mode
<code>access-list arp</code>	Creates a ARP ACL and enters configuration mode	GC
<code>permit, deny</code>	Filters packets matching a specified source or destination address in ARP messages	ARP-ACL
<code>show access-list arp</code>	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 \(367\)](#)

[show access-list arp \(368\)](#)

**permit, deny (ARPA CL)** 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*<sup>7</sup> – IPv4 number representing the address bits to match.

*source-mac* – Source MAC address.

*destination-mac* – Destination MAC address range with bitmask.

*mac-address-bitmask*<sup>7</sup> – Bitmask for MAC address (in hexadecimal format).

**log** - Logs a packet when it matches the access control entry.

### Default Setting

None

### Command Mode

ARP ACL

### Command Usage

New rules are added to the end of the list.

7. For all bitmasks, binary “1” means relevant and “0” means ignore.

### 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 \(366\)](#)

**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 \(367\)](#)

---

## ACL Information

This section describes commands used to display ACL information.

**Table 72: ACL Information Commands**

Command	Function	Mode
<a href="#">clear access-list hardware counters</a>	Clears hit counter for rules in all ACLs, or in a specified ACL	PE
<a href="#">show access-group</a>	Shows the ACLs assigned to each port	PE
<a href="#">show access-list</a>	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: 1-26/28/52)

*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 or egress rules for ARP ACLs.

**hardware counters** – Shows statistics for all ACLs.<sup>8</sup>

**ip extended** – Shows ingress or egress rules for Extended IPv4 ACLs.

**ip standard** – Shows ingress or egress rules for Standard IPv4 ACLs.

**ipv6 extended** – Shows ingress or egress rules for Extended IPv6 ACLs.

**ipv6 standard** – Shows ingress or egress rules for Standard IPv6 ACLs.

**mac** – Shows ingress or egress rules 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 73: 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>discard</code>	Discards CDP or PVST packets	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

**Table 73: Interface Commands** (Continued)

Command	Function	Mode
<code>transceiver-threshold current</code>	Sets thresholds for transceiver current which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold rx-power</code>	Sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold temperature</code>	Sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold tx-power</code>	Sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold voltage</code>	Sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message	IC
<code>show interfaces transceiver</code>	Displays the temperature, voltage, bias current, transmit power, and receive power	PE
<code>show interfaces transceiver-threshold</code>	Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power	PE
<i>Cable Diagnostics</i>		
<code>test cable-diagnostics</code>	Performs cable diagnostics on the specified port	PE
<code>show cable-diagnostics</code>	Shows the results of a cable diagnostics test	PE
<i>Power Savings</i>		
<code>power-save</code>	Enables power savings mode on the specified port	IC
<code>show power-save</code>	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.

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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

- ◆ 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.
- ◆ 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 \(377\)](#)

[speed-duplex \(379\)](#)

[flowcontrol \(375\)](#)

**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)#
```

**discard** This command discards CDP or PVST packets. Use the **no** form to forward the specified packet type to other ports configured the same way.

### Syntax

**[no] discard { cdp | pvst }**

**cdp** – Cisco Discovery Protocol

**pvst** – Per-VLAN Spanning Tree

### Default Setting

Default - Forward CDP and PVST packets

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

Use the **no discard** command to allow CDP or PVST packets to be forwarded to other ports in the same VLAN which are also configured to forward the specified packet type.

### EXAMPLE

The following example forwards CDP packets entering port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no discard cdp
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 \(377\)](#)

[capabilities \(373\)](#)

**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.

**Default Setting**

SFP+ ports: None

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

Available sfp-forced modes include:

ECS4100-26TX:	Ports 25-26 (1000BASE SFP) support 1000sfp
ECS4100-26TX-ME:	Ports 25-26 (1000BASE SFP) support 1000sfp
ECS4100-28T:	Ports 25-28 (1000BASE SFP) support 1000sfp
ECS4100-52T:	Ports 49-52 (1000BASE SFP) support 1000sfp

**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 \(373\)](#)

[speed-duplex \(379\)](#)

**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 \(377\)](#)

[capabilities \(373\)](#)

**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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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
:

```

**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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 74: 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.
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.

**Table 74: show interfaces counters - display description** (Continued)

Parameter	Description
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 exceeded the maximum permitted frame size.
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present.  For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII.  For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII
<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.
CRC Align Errors	
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	



**Table 74: show interfaces counters - display description** (Continued)

Parameter	Description
<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.
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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

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

*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

Discards      Errors
-----
                41                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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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)
Forbidden VLAN          :
Console#
```

**Table 75: 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 ( <a href="#">page 427</a> ).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level ( <a href="#">page 427</a> ).

**Table 75: show interfaces switchport - display description** (Continued)

Field	Description
Unknown Unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 427).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 405).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 1023).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 485).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 485).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 483).
Native VLAN	Indicates the default Port VLAN ID (page 486).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 556).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 483).
Forbidden VLAN	Shows the VLANs this interface can not join (page 476).

## 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: 25-26/25-28/49-52)

### 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: 25-26/25-28/49-52)

### 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 dsp interface** *interface*

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-22/24/48)

### Command Mode

Privileged Exec

### Command Usage

- ◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test method when the port link-up speed is 1 Gbps. DSP 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. 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 dsp interface** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-22/24/48)

### 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 0n 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 1-22/24/48)

### Command Usage

- ◆ IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.
- ◆ 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 cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to

determine whether or not it can reduce the signal amplitude used on a particular link.



**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: 1-22/24/48)

### 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 16 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 76: 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 status port-channel</code>	Shows 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: 1-16)

### 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: 1-16)

**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 77: 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 77: 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
Port Channel : 1
Admin Key    : 0
Oper Key     : 4
Timeout      : Long
-----
Member Port   : Eth 1/24
Periodic Time : 30 seconds
System Priority : 32768
Port Priority  : 32768
Admin Key     : 4
Oper Key      : 4
Admin State   : Defaulted, Aggregatable, Long Timeout, Active LACP
Oper State    : Distributing, Collecting, Synchronization, Aggregatable,
                Long Timeout, Active LACP
:

```

**Table 78: 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"> <li>◆ Expired – The actor's receive machine is in the expired state;</li> <li>◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner.</li> <li>◆ 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.</li> <li>◆ 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.</li> <li>◆ 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.</li> </ul>

**Table 78: show lacp internal - display description** (Continued)

Field	Description
Admin State, Oper State (continued)	<ul style="list-style-type: none"> <li>◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation.</li> <li>◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate.</li> <li>◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)</li> </ul>

```

Console#show lacp 1 neighbors
Port Channel : 1
-----
Member Port           : Eth 1/24
Partner Admin System ID : 32768, 00-00-00-00-00-00
Partner Oper System ID : 32768, FC-0A-81-B7-C7-E0
Partner Admin Port ID  : 32768, 24
Partner Oper Port ID   : 32768, 24
Partner Admin Key      : 0
Partner Oper Key       : 4
Partner Admin State    : Defaulted, Distributing, Collecting,
                        Synchronization, Long Timeout, Passive LACP
Partner Oper State     : Distributing, Collecting, Synchronization,
                        Aggregatable, Long Timeout, Active LACP
:

```

**Table 79: 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 ID	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.
Partner Admin Key	Current administrative value of the Key for the protocol partner.
Partner Oper Key	Current operational value of the Key for the protocol partner.
Partner Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Partner 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 80: 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#
```

# 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 81: 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 82: Mirror Port Commands**

Command	Function	Mode
<code>port monitor</code>	Configures a mirror session	IC
<code>show port monitor</code>	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] | vlan vlan-id |
mac-address mac-address | access-list acl-name}
```

```
no port monitor {interface | vlan vlan-id |
mac-address mac-address | access-list acl-name}
```

*interface* - **ethernet** *unit/port* (source port)

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**rx** - Mirror received packets.

**tx** - Mirror transmitted packets.

**both** - Mirror both received and transmitted packets.

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

*mac-address* - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

*acl-name* – Name of the ACL. (Maximum length: 32 characters, no spaces or other special characters)

### Default Setting

- ◆ No mirror session is defined.
- ◆ When enabled for an interface, default mirroring is for both received and transmitted packets.
- ◆ When enabled for a VLAN or a MAC address, mirroring is restricted to received 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. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- ◆ When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirror VLAN.
- ◆ When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.
- ◆ Spanning Tree BPDU packets are not mirrored to the target port.
- ◆ When mirroring VLAN traffic or packets based on a source MAC address, the target port cannot be set to the same target port as that used for basic port mirroring.
- ◆ 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.
- ◆ ACL-based mirroring is only used for ingress traffic. To mirror an ACL, follow these steps:
  1. Use the **access-list** command to add an ACL.
  2. Use the **access-group** command to add a mirrored port to access control list.
  3. Use the **port monitor access-list** command to specify the destination port to which traffic matching the ACL will be mirrored.

### 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)#
```

This example configures port 2 to monitor packets matching the MAC address 00-12-CF-XX-XX-XX received by port 1:

```
Console(config)#access-list mac m1
Console(config-mac-acl)#permit 00-12-cf-00-00-00 ff-ff-ff-00-00-00 any
Console(config-mac-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#mac access-group m1 in
Console(config-if)#interface ethernet 1/2
Console(config-if)#port monitor access-list m1
Console(config-if)#
```

**show port monitor** This command displays mirror information.

### Syntax

```
show port monitor [interface | vlan vlan-id | mac-address mac-address |  
access-list acl-name]
```

*interface* - **ethernet** *unit/port* (source port)

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

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

*mac-address* - MAC address in the form of xx-xx-xx-xx-xx-xx or  
xxxxxxxxxxxx.

*acl-name* – Name of the ACL. (Maximum length: 32 characters, no spaces or other special characters)

### 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 83: 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: 1-26/28/52)

**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: 1-26/28/52)

**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: 1-26/28/52)

### 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. Nor can GVRP dynamically add port members to an RSPAN VLAN. 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 84: Congestion Control Commands**

Command Group	Function
<a href="#">Rate Limiting</a>	Sets the input and output rate limits for a port.
<a href="#">Storm Control</a>	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 85: Rate Limit Commands**

Command	Function	Mode
<a href="#">rate-limit</a>	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)

### 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.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

### Related Command

[show interfaces switchport \(388\)](#)

## 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 86: Rate Limit Commands**

Command	Function	Mode
<code>switchport packet-rate</code>	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
<code>show interfaces switchport</code>	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 \(388\)](#)

# 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 87: 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 an 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

Disabled

#### 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 {block | none | shutdown}**

**no loopback-detection action**

**block** - When a loopback is detected on a port which a member of a specific VLAN, packets belonging to that VLAN are dropped at the offending port.

**none** - No action is taken.

**shutdown** - Shuts down the interface.

#### Default Setting

Shut down

#### Command Mode

Global Configuration

### Command Usage

- ◆ When the response to a detected loopback condition is set to block user traffic, loopback detection control frames may be untagged or tagged depending on the port's VLAN membership type.
- ◆ When the response to a detected loopback condition is set to block user traffic, ingress filtering for the port is enabled automatically if not already enabled by the `switchport ingress-filtering` command. The port's original setting for ingress filtering will be restored when loopback detection is disabled.
- ◆ When a port receives a control frame sent by itself, this means that the port is in a looped state, and the VLAN in the frame payload is also in a 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: 1-26/28/52)

### 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 88: 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 collision-mac-address-table</code>	Removes all entries from the collision MAC address table	PE
<code>clear mac-address-table dynamic</code>	Removes any learned entries from the forwarding database	PE
<code>show collision-mac-address-table</code>	Shows a shows a list of MAC addresses that cannot be learned by the switch due to hash collisions	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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

*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 collision-mac-address-table** This command removes all entries from the collision MAC address table.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```
Console#clear collision-mac-address-table
Console#
```

**clear mac-address-table dynamic** This command removes any learned entries from the forwarding database.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Command Usage**

Even if a hash collision for a MAC address is resolved, entries in collision 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
Console#
```

**show collision-mac-address-table** This command shows a list of MAC addresses that cannot be learned by the switch due to hash collisions.

**Command Mode**

Privileged Exec

**Example**

```

Console#show collision-mac-address-table
MAC Address          VLAN  Collision Count
-----
90-e6-ba-cb-cd-d6    1          2
Total collision mac number: 1
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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

*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 16K.

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 89: 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 89: 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 restricted-tcn</code>	Prevents a TCN from being propagated from an aggregation switch to the uplink port on access switches	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
<code>show spanning-tree tc-prop</code>	Shows configuration of topology change propagation domains	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 \(444\)](#)

[spanning-tree max-age \(445\)](#)

**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 \(444\)](#)

[spanning-tree hello-time \(444\)](#)

**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 \(452\)](#)  
[mst priority \(451\)](#)  
[name \(453\)](#)  
[revision \(453\)](#)  
[max-hops \(451\)](#)

### 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 456) takes precedence over port priority (page 464).
- ◆ 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
Console(config)#
```

**spanning-tree tc-prop** This command configures a topology change propagation domain. Use the **no** form to remove a propagation domain.

### Syntax

**spanning-tree tc-prop group** *group-id* {**ethernet** *interface* | **port-channel** *trunk-id*}

*group-id* - Group identifier. (Range: 1-255)

*interface* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

*trunk-id* - Trunk index (Range: 1-16)

### Default Setting

All ports and trunks belong to a common group.

### Command Mode

Global Configuration

### Command Usage

A port can only belong to one group. When an interface is added to a group, it is removed from the default group. When a TCN BPDU or BPDU with the TC flag set is received on an interface, that interface will only notify members in same group to propagate this topology change.

### Example

```
Console(config)#spanning-tree tc-prop group 1 ethernet 1/1-5
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*

*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 453](#)) 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*

*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 453](#)) 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 \(453\)](#)

**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*

*number* - Revision number of the spanning tree. (Range: 0-65535)

### Default Setting

0

### Command Mode

MST Configuration

### Command Usage

The MST region name ([page 453](#)) 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 \(453\)](#)

**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 bpd-filter
Console(config-if)#
```

### Related Commands

[spanning-tree edge-port \(457\)](#)

**spanning-tree bpduguard** 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 bpduguard** [**auto-recovery** [**interval** *interval*]]

**no spanning-tree bpduguard** [**auto-recovery** [**interval**]]

**auto-recovery** - Automatically re-enables an interface after the specified interval.

*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 bpduguard
Console(config-if)#
```

### Related Commands

[spanning-tree edge-port \(457\)](#)

[spanning-tree spanning-disabled \(466\)](#)

**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)<sup>9</sup>

**Table 90: 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
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 91: 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.

9. 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).



- ◆ Path cost takes precedence over port priority.
- ◆ When the path cost method ([page 447](#)) 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)#
```

**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

Enabled

#### 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 {block | 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, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
  - The port receives any other BPDU except for its own, or;
  - The port's link status changes to link down and then link up again, or;
  - The port ceases to receive its own BPDUs in a forward delay interval.
- ◆ 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 restricted-tcn** This command prevents a TCN from being propagated from an aggregation switch to the uplink port on access switches. Use the **no** form to restore the default setting.

#### Syntax

**[no] spanning-tree restricted-tcn**

#### Default Setting

Disabled

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

This command prevents an aggregation switch from propagating Topology Change Notifications (TCNs), from to the uplink port on access switches. In other words, TCNs are filtering on all neighboring rings attached to access switches.

#### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree restricted-tcn
```

**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 method<sup>10</sup>, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in [Table 90 on page 456](#).

### 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 91 on page 456](#).

### 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 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 \(463\)](#)

<sup>10</sup>. Use the [spanning-tree pathcost method](#) command to set the path cost method.

**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 \(462\)](#)

**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 \(456\)](#)

**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 edge-port
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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

#### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

*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
Restricted TCN                     : 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
-----
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#

```

**show spanning-tree tc-prop** This command shows the configuration of topology change propagation domains.

#### Syntax

**show spanning-tree tc-prop [group *group-id*]**

*group-id* - Group identifier. (Range: 1-255)

#### Command Mode

Privileged Exec

#### Example

```
Console#show spanning-tree tc-prop group 1
Group 1
  Eth 1/ 1, Eth 1/ 2, Eth 1/ 3, Eth 1/ 4, Eth 1/ 5
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 92: VLAN Commands**

Command Group	Function
<a href="#">GVRP and Bridge Extension Commands</a>	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB
<a href="#">Editing VLAN Groups</a>	Sets up VLAN groups, including name, VID and state
<a href="#">Configuring VLAN Interfaces</a>	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, and PVID
<a href="#">Displaying VLAN Information</a>	Displays VLAN groups, status, port members, and MAC addresses
<a href="#">Configuring IEEE 802.1Q Tunneling</a>	Configures 802.1Q Tunneling (QinQ Tunneling)
<a href="#">Configuring L2PT Tunneling</a>	Configures Layer 2 Protocol Tunneling (L2PT), either by discarding, processing, or transparently passing control packets across a QinQ tunnel
<a href="#">Configuring VLAN Translation<sup>1</sup></a>	Maps VLAN ID between customer and service provider for networks that do not support IEEE 802.1Q tunneling
<a href="#">Configuring Protocol-based VLANs<sup>1</sup></a>	Configures protocol-based VLANs based on frame type and protocol
<a href="#">Configuring IP Subnet VLANs<sup>1</sup></a>	Configures IP Subnet-based VLANs
<a href="#">Configuring MAC Based VLANs<sup>1</sup></a>	Configures MAC-based VLANs
<a href="#">Configuring Voice VLANs</a>	Configures VoIP traffic detection and enables a Voice VLAN

<sup>1</sup> 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, IP subnet-based, protocol-based, and then native port-based (see the [switchport priority default](#) command).

## GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

**Table 93: GVRP and Bridge Extension Commands**

Command	Function	Mode
<code>bridge-ext gvrp</code>	Enables GVRP globally for the switch	GC
<code>garp timer</code>	Sets the GARP timer for the selected function	IC
<code>switchport forbidden vlan</code>	Configures forbidden VLANs for an interface	IC
<code>switchport gvrp</code>	Enables GVRP for an interface	IC
<code>show bridge-ext</code>	Shows the global bridge extension configuration	PE
<code>show garp timer</code>	Shows the GARP timer for the selected function	NE, PE
<code>show gvrp configuration</code>	Displays GVRP configuration for the selected interface	NE, PE

**bridge-ext gvrp** This command enables GVRP globally for the switch. Use the **no** form to disable it.

### Syntax

**[no] bridge-ext gvrp**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

### Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

**garp timer** This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

### Syntax

**garp timer {join | leave | leaveall} timer-value**

**no garp timer {join | leave | leaveall}**

**{join | leave | leaveall}** - Timer to set.

*timer-value* - Value of timer.

Ranges:

join: 20-1000 centiseconds

leave: 60-3000 centiseconds

leaveall: 500-18000 centiseconds

### Default Setting

join: 20 centiseconds

leave: 60 centiseconds

leaveall: 1000 centiseconds

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
  
- ◆ Timer values must meet the following restrictions:
  - leave > (2 x join)
  - leaveall > leave



**Note:** Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

### Related Commands

[show garp timer \(478\)](#)

**switchport forbidden vlan** This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

### Syntax

**switchport forbidden vlan** {**add** *vlan-list* | **remove** *vlan-list*}

**no switchport forbidden vlan**

**add** *vlan-list* - List of VLAN identifiers to add.

**remove** *vlan-list* - List of VLAN identifiers to remove.

*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

No VLANs are included in the forbidden list.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ This command prevents a VLAN from being automatically added to the specified interface via GVRP using the **switchport gvrp** command or added manually using the **switchport allowed vlan** command.
- ◆ If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.
- ◆ GVRP cannot be enabled for ports set to Access mode (see the **switchport mode** command).
- ◆ This command will not be accepted if the specified VLAN does not exist on the switch.

### Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

**switchport gvrp** This command enables GVRP for a port. Use the **no** form to disable it.

### Syntax

**[no] switchport gvrp**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

GVRP cannot be enabled for ports set to Access mode using the [switchport mode](#) command.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

**show bridge-ext** This command shows the configuration for bridge extension commands.

### Default Setting

None

### Command Mode

Privileged Exec

### Example

```
Console#show bridge-ext
Maximum Supported VLAN Numbers      : 4094
Maximum Supported VLAN ID           : 4094
Extended Multicast Filtering Services : No
Static Entry Individual Port         : Yes
VLAN Version Number                  : 2
VLAN Learning                        : IVL
Configurable PVID Tagging            : Yes
Local VLAN Capable                   : No
Traffic Classes                      : Enabled
Global GVRP Status                   : Disabled
Console#
```

**Table 94: show bridge-ext - display description**

Field	Description
Maximum Supported VLAN Numbers	The maximum number of VLANs supported on this switch.
Maximum Supported VLAN ID	The maximum configurable VLAN identifier supported on this switch.
Extended Multicast Filtering Services	This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).

**Table 94: show bridge-ext - display description** (Continued)

Field	Description
Static Entry Individual Port	This switch allows static filtering for unicast and multicast addresses. (Refer to the <a href="#">mac-address-table static</a> command.)
VLAN Version Number	Based on IEEE 802.1Q, "1" indicates Bridges that support only single spanning tree (SST) operation, and "2" indicates Bridges that support multiple spanning tree (MST) operation.
VLAN Learning	This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
Configurable PVID Tagging	This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to the <a href="#">switchport allowed vlan</a> command.)
Local VLAN Capable	This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
Traffic Classes	This switch provides mapping of user priorities to multiple traffic classes. (Refer to " <a href="#">Class of Service Commands</a> " on page 553.)
Global GVRP Status	GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This field shows if GVRP is globally enabled or disabled. (Refer to the <a href="#">bridge-ext gvrp</a> command.)

**show garp timer** This command shows the GARP timers for the selected interface.

### Syntax

**show garp timer** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### Default Setting

Shows all GARP timers.

### Command Mode

Normal Exec, Privileged Exec

### Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
  Join Timer       : 20 centiseconds
  Leave Timer      : 60 centiseconds
  Leave All Timer  : 1000 centiseconds
Console#
```

### Related Commands

[garp timer \(475\)](#)

**show gvrp configuration** This command shows if GVRP is enabled.

#### Syntax

```
show gvrp configuration [interface]
    interface
        ethernet unit/port
            unit - Unit identifier. (Range: 1)
            port - Port number. (Range: 1-26/28/52)
        port-channel channel-id (Range: 1-16)
```

#### Default Setting

Shows both global and interface-specific configuration.

#### Command Mode

Normal Exec, Privileged Exec

#### Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
  GVRP Configuration : Disabled
Console#
```

## Editing VLAN Groups

Table 95: Commands for Editing VLAN Groups

Command	Function	Mode
<a href="#">vlan database</a>	Enters VLAN database mode to add, change, and delete VLANs	GC
<a href="#">vlan</a>	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 \(487\)](#)

**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 418.





**Note:** Ports can only be added to an RSPAN VLAN using the commands described under “RSPAN Mirroring Commands”.

### 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 \(487\)](#)

## Configuring VLAN Interfaces

Table 96: Commands for Configuring VLAN Interfaces

Command	Function	Mode
<a href="#">interface vlan</a>	Enters interface configuration mode for a specified VLAN	IC
<a href="#">switchport acceptable-frame-types</a>	Configures frame types to be accepted by an interface	IC
<a href="#">switchport allowed vlan</a>	Configures the VLANs associated with an interface	IC
<a href="#">switchport forbidden vlan</a>	Configures forbidden VLANs for an interface	IC
<a href="#">switchport gvrp</a>	Enables GVRP for an interface	IC
<a href="#">switchport ingress-filtering</a>	Enables ingress filtering on an interface	IC
<a href="#">switchport mode</a>	Configures VLAN membership mode for an interface	IC

Table 96: Commands for Configuring VLAN Interfaces (Continued)

Command	Function	Mode
<a href="#">switchport native vlan</a>	Configures the PVID (native VLAN) of an interface	IC
<a href="#">switchport priority default</a>	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 \(378\)](#)

[interface \(372\)](#)

[vlan \(480\)](#)

**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 \(485\)](#)

**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.
- ◆ Ports can only be added to an RSPAN VLAN using the commands described under "[RSPAN Mirroring Commands](#)".

### 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 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 GVRP or 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

All ports are in 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 \(483\)](#)

**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 97: 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 the commands used to configure QinQ tunneling.

**Table 98: 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>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>switchport dot1q-tunnel service default match all discard</code>	Configures an interface to discard all traffic entering the QinQ tunnel access port	IC
<code>switchport dot1q-tunnel service default match untagged discard</code>	Configures an interface to discard untagged traffic entering or exiting a dot1q-tunnel service VLAN	IC
<code>switchport dot1q-tunnel service match cvid</code>	Creates a CVLAN to SPVLAN mapping entry	IC
<code>switchport dot1q-tunnel tpid</code>	Sets the Tag Protocol Identifier (TPID) value of a tunnel port	IC
<code>show dot1q-tunnel service</code>	Displays tunnel service subscriptions, default discard service, and discarded untagged traffic configuration	PE
<code>show dot1q-tunnel</code>	Displays the configuration of QinQ tunnel ports	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. Configure the QinQ tunnel access port to dot1Q-tunnel access mode ([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 [switchport 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 \(497\)](#)

[show interfaces switchport \(388\)](#)

**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 \(497\)](#)

[show interfaces switchport \(388\)](#)

### **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)#
```

### **switchport dot1q-tunnel service default match all discard**

This command discards all traffic that does not match any other dot1q-tunnel service settings. Use the **no** form to restore the default setting.

### Syntax

**[no] switchport dot1q-tunnel service match all discard**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service match all discard
Console(config-if)#
```

**switchport dot1q-tunnel service default match untagged discard** This command discards untagged traffic entering the QinQ tunnel access port. Use the **no** form to restore the default setting.

### Syntax

**[no] switchport dot1q-tunnel service default match untagged discard**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service match untagged discard
Console(config-if)#
```

**switchport dot1q-tunnel service match cvid** This command creates a CVLAN to SPVLAN mapping entry. Use the **no** form to delete a VLAN mapping entry.

### Syntax

**switchport dot1q-tunnel service svid match cvid cvid [remove-ctag]**

**no switchport dot1q-tunnel service [svid [match cvid cvid]]**

*svid* - VLAN ID for the outer VLAN tag (Service Provider VID). (Range: 1-4094)

*cvid* - VLAN ID for the inner VLAN tag (Customer VID). (Range: 1-4094)

### Default Setting

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ The inner VLAN tag of a customer packet entering the edge router of a service provider's network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. This process is performed in a transparent manner.

- ◆ 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.
- ◆ Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider's network for traffic arriving from specified inbound customer VLANs.
- ◆ Note that all customer interfaces should be configured as access interfaces (that is, a user-to-network interface) and service provider interfaces as uplink interfaces (that is, a network-to-network interface). Use the `switchport dot1q-tunnel mode uplink` command to set an interface to access or uplink mode.
- ◆ When the **remove-ctag** option is specified, the inner-tag containing the customer's VID is removed, and the outer-tag containing the service provider's VID remains in place.

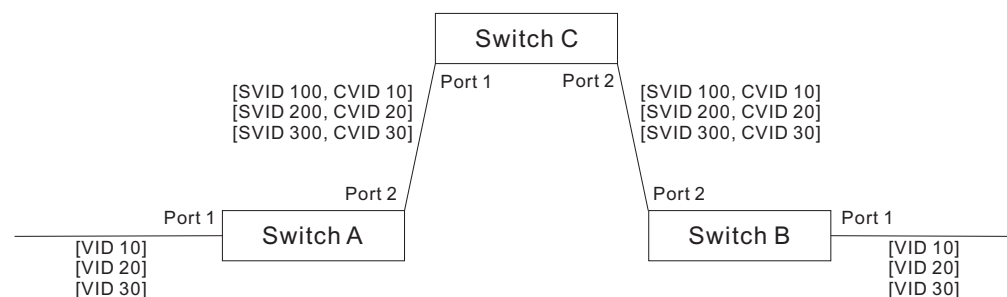
### Example

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2
Console(config-if)#
```

The following example maps C-VLAN 10 to S-VLAN 100, C-VLAN 20 to S-VLAN 200 and C-VLAN 30 to S-VLAN 300 for ingress traffic on port 1 of Switches A and B.

**Figure 1: Mapping QinQ Service VLAN to Customer VLAN**



Step 1. Configure Switch A and B.

**1. Create VLANs 100, 200 and 300.**

```
Console(config)#vlan database
Console(config-vlan)#vlan 100,200,300 media ethernet state active
```

**2. Enable QinQ.**

```
Console(config)#dot1q-tunnel system-tunnel-control
```

3. Configure port 2 as a tagged member of VLANs 100, 200 and 300 using uplink mode.

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 100,200,300 tagged
Console(config-if)#switchport dot1q-tunnel mode uplink
```

4. Configures port 1 as an untagged member of VLANs 100, 200 and 300 using access mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 100,200,300 untagged
Console(config-if)#switchport dot1q-tunnel mode access
```

5. Configure the following selective QinQ mapping entries.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 100 match cvid 10
Console(config-if)#switchport dot1q-tunnel service 200 match cvid 20
Console(config-if)#switchport dot1q-tunnel service 300 match cvid 30
```

6. Configures port 1 as member of VLANs 10, 20 and 30 to avoid filtering out incoming frames tagged with VID 10, 20 or 30 on port 1

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 10,20,30
```

7. Verify configuration settings.

```
Console#show dot1q-tunnel service
802.1Q Tunnel Service Subscriptions

  Port      Match C-VID S-VID Remove C-Tag
  -----
Eth 1/ 1      10   100 Disabled
Eth 1/ 1      20   200 Disabled
Eth 1/ 1      30   300 Disabled

Default Service

  Port      Discard
  -----
Eth 1/ 1 Enabled

Discard Untagged Traffic

  Port
  -----
Eth 1/ 1
```

## Step 2. Configure Switch C.

1. Create VLAN 100, 200 and 300.

```
Console(config)#vlan database
Console(config-vlan)#vlan 100,200,300 media ethernet state active
```

2. Configure port 1 and port 2 as tagged members of VLAN 100, 200 and 300.

```
Console(config)#interface ethernet 1/1,2
Console(config-if)#switchport allowed vlan add 100,200,300 tagged
```

**switchport dot1q-tunnel tpid** This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

### Syntax

**switchport dot1q-tunnel tpid** *tpid*

**no switchport dot1q-tunnel tpid**

*tpid* – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

### Default Setting

0x8100

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. 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, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that 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 8100. If the port is in Access mode, received packets are processed as untagged packets.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

### Related Commands

[show interfaces switchport \(388\)](#)

**show dot1q-tunnel service** This command shows tunnel service subscriptions, default discard service, and discarded untagged traffic configuration.

### Syntax

**show dot1q-tunnel service** [*svid* | **default**]

*svid* - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094)

**default** - Shows the default discard service, and discarded untagged traffic configuration

### Command Mode

Privileged Exec

### Example

```
Console(config)#show dot1q-tunnel service
802.1Q Tunnel Service Subscriptions

Port      Match C-VID S-VID Remove C-Tag
-----
Eth 1/ 1          1      1 Disabled

Default Service

Port      Discard
-----
Eth 1/ 1 Enabled

Discard Untagged Traffic

Port
-----
Eth 1/ 1

Console(config)#show dot1q-tunnel service 100
802.1Q Tunnel Service Subscriptions

Port      Match C-VID S-VID Remove C-Tag
-----
Eth 1/ 5          1     100

Default Service

Port      Discard
-----

Discard Untagged Traffic

Port
-----

Console(config)#show dot1q-tunnel service default
802.1Q Tunnel Service Subscriptions

Default Service

Port      Discard
-----
```



```
Discard Untagged Traffic
```

```
Port
-----
```

```
Console#
```

**show dot1q-tunnel** This command displays information about QinQ tunnel ports.

### Syntax

```
show dot1q-tunnel [interface interface [service svid] | service [svid]]
```

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

*svid* - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094)

### Command Mode

Privileged Exec

### Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel
802.1Q Tunnel Status : Enabled
802.1Q Tunnel TPID   : 8100 (Hex)

Port      Mode      Priority Mapping
-----
Eth 1/ 1 Access Disabled
Eth 1/ 2 Uplink Disabled
Eth 1/ 3 Normal Disabled
:
:
Console#show dot1q-tunnel interface ethernet 1/5
802.1Q Tunnel Service Subscriptions

Port      Match C-VID S-VID Remove C-Tag
-----
Eth 1/ 5           1   100

Default Service

Port      Discard
-----
```

```
Discard Untagged Traffic

Port
-----

Console#show dot1q-tunnel service 100
802.1Q Tunnel Service Subscriptions

Port      Match C-VID S-VID Remove C-Tag
-----
Eth 1/ 5          1   100
Eth 1/ 6          1   100

Console#
```

### Related Commands

[switchport dot1q-tunnel mode \(490\)](#)

## Configuring L2PT Tunneling

This section describes the commands used to configure Layer 2 Protocol Tunneling (L2PT).

**Table 99: L2 Protocol Tunnel Commands**

Command	Function	Mode
<a href="#">l2protocol-tunnel tunnel-dmac</a>	Configures the destination address for Layer 2 Protocol Tunneling	GC
<a href="#">switchport l2protocol-tunnel</a>	Enables Layer 2 Protocol Tunneling for the specified protocol	IC
<a href="#">show l2protocol-tunnel</a>	Shows settings for Layer 2 Protocol Tunneling	PE

**[l2protocol-tunnel tunnel-dmac](#)** This command configures the destination address for Layer 2 Protocol Tunneling (L2PT). Use the **no** form to restore the default setting.

### Syntax

**[l2protocol-tunnel tunnel-dmac](#) *mac-address***

*mac-address* – The switch rewrites the destination MAC address in all upstream L2PT protocol packets (i.e, STP BPDUs) to this value, and forwards them on to uplink ports. The MAC address must be specified in the format `xx-xx-xx-xx-xx-xx` or `xxxxxxxxxxxx`.

### Default Setting

01-12-CF-.00-00-02, proprietary tunnel address

### Command Mode

Global Configuration

### Command Usage

- ◆ When L2PT is not used, protocol packets (such as STP) are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer's network.
- ◆ L2PT can be used to pass various types of protocol packets belonging to the same customer transparently across a service provider's network. In this way, normally segregated network segments can be configured to function inside a common protocol domain.
- ◆ L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address (for example, the spanning tree protocol uses 10-12-CF-00-00-02), a reserved address for other specified protocol types (as defined in IEEE 802.1ad – Provider Bridges), or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site (via all of the appropriate tunnel ports and access ports<sup>11</sup> connected to the same metro VLAN).
- ◆ The way in which L2PT processes packets is based on the following criteria – (1) packet is received on a QinQ uplink port, (2) packet is received on a QinQ access port, or (3) received packet is Cisco-compatible L2PT (i.e., as indicated by a proprietary MAC address).

### *Processing protocol packets defined in IEEE 802.1ad – Provider Bridges*

- ◆ When an IEEE 802.1ad protocol packet is received on an uplink port (i.e., an 802.1Q tunnel ingress port connecting the edge switch to the service provider network)
  - with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN tag), it is forwarded to all QinQ uplink ports and QinQ access ports in the same S-VLAN for which L2PT is enabled for that protocol.
  - with the destination address 01-80-C2-00-00-01~0A (S-VLAN tag), it is filtered, decapsulated, and processed locally by the switch if the protocol is supported.
- ◆ When a protocol packet is received on an access port (i.e., an 802.1Q trunk port connecting the edge switch to the local customer network)
  - with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN), and
    - L2PT is enabled on the port, the frame is forwarded to all QinQ uplink ports and QinQ access ports on which L2PT is enabled for that protocol in the same S-VLAN.

11. Access ports in this context are 802.1Q trunk ports.

- L2PT is disabled on the port, the frame is decapsulated and processed locally by the switch if the protocol is supported.
- with destination address 01-80-C2-00-00-01~0A (S-VLAN), the frame is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

*Processing Cisco-compatible protocol packets*

- ◆ When a Cisco-compatible L2PT packet is received on an uplink port, and
  - recognized as a CDP/VTP/STP/PVST+ protocol packet (where STP means STP/RSTP/MSTP), it is forwarded to the following ports in the same S-VLAN: (a) all access ports for which L2PT has been disabled, and (b) all uplink ports.
  - recognized as a Generic Bridge PDU Tunneling (GBPT) protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), it is forwarded to the following ports in the same S-VLAN:
    - other access ports for which L2PT is enabled after decapsulating the packet and restoring the proper protocol and MAC address information.
    - all uplink ports.
- ◆ When a Cisco-compatible L2PT packet is received on an access port, and
  - recognized as a CDP/VTP/STP/PVST+ protocol packet, and
    - L2PT is enabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is enabled, and (b) uplink ports after rewriting the destination address to make it a GBPT protocol packet (i.e., setting the destination address to 01-00-0C-CD-CD-D0).
    - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
  - recognized as a GBPT protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), and
    - L2PT is enabled on this port, it is forwarded to other access ports in the same S-VLAN for which L2PT is enabled
    - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.

- ◆ For L2PT to function properly, QinQ must be enabled on the switch using the [dot1q-tunnel system-tunnel-control](#) command, and the interface configured to 802.1Q tunnel mode using the [switchport dot1q-tunnel mode](#) command.

### Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#l2protocol-tunnel tunnel-dmac 01-80-C2-00-00-01
Console(config-)#
```

**switchport l2protocol-tunnel** This command enables Layer 2 Protocol Tunneling (L2PT) for the specified protocol. Use the **no** form to disable L2PT for the specified protocol.

### Syntax

**switchport l2protocol-tunnel {cdp | lacp | lldp | pvst+ | spanning-tree | vtp}**

**cdp** - Cisco Discovery Protocol

**lacp** - Link Aggregation Control Protocol

**lldp** - Link Layer Discovery Protocol

**pvst+** - Cisco Per VLAN Spanning Tree Plus

**spanning-tree** - Spanning Tree (STP, RSTP, MSTP)

**vtp** - Cisco VLAN Trunking Protocol

### Default Setting

Disabled for all protocols

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Refer to the Command Usage section for the [l2protocol-tunnel tunnel-dmac](#) command.
- ◆ For L2PT to function properly, QinQ must be enabled on the switch using the [dot1q-tunnel system-tunnel-control](#) command, and the interface configured to 802.1Q tunnel mode using the [switchport dot1q-tunnel mode](#) command.

### Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#switchport l2protocol-tunnel spanning-tree
Console(config-if)#
```

**show l2protocol-tunnel** This command shows settings for Layer 2 Protocol Tunneling (L2PT).

**Command Mode**  
Privileged Exec

#### Example

```
Console#show l2protocol-tunnel
Layer 2 Protocol Tunnel

Tunnel MAC Address : 01-12-CF-00-00-00

Interface Protocol
-----
Eth 1/ 1    Spanning Tree

Console#
```

## Configuring VLAN Translation

QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the switches directly connected to that device can be configured to swap the customer's VLAN ID with the service provider's VLAN ID for upstream traffic, or the service provider's VLAN ID with the customer's VLAN ID for downstream traffic.

This section describes commands used to configure VLAN translation.

**Table 100: VLAN Translation Commands**

Command	Function	Mode
<a href="#">switchport vlan-translation</a>	Maps VLAN IDs between the customer and service provider	IC
<a href="#">show vlan-translation</a>	Displays the configuration settings for VLAN translation	PE

**switchport vlan-translation** This command maps VLAN IDs between the customer and service provider.

#### Syntax

**switchport vlan-translation** *original-vlan new-vlan*

**no switchport vlan-translation** *original-vlan*

*original-vlan* - The original VLAN ID. (Range: 1-4094)

*new-vlan* - The new VLAN ID. (Range: 1-4094)

#### Default Setting

Disabled

## Command Mode

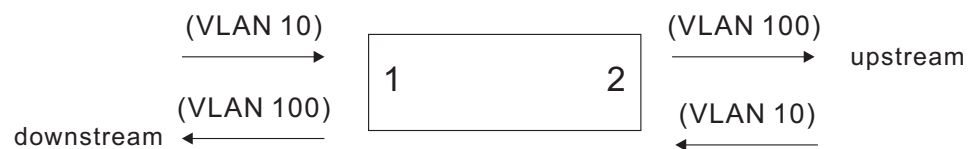
Interface Configuration (Ethernet)

## Command Usage

- ◆ If the next switch upstream does not support QinQ tunneling, then use this command to map the customer's VLAN ID to the service provider's VLAN ID for the upstream port. Similarly, if the next switch downstream does not support QinQ tunneling, then use this command to map the service provider's VLAN ID to the customer's VLAN ID for the downstream port. Note that one command maps both the *original-vlan* to *new-vlan* for ingress traffic and the *new-vlan* to *original-vlan* for egress traffic on the specified port.

For example, assume that the upstream switch does not support QinQ tunneling. If the command **switchport vlan-translation 10 100** is used to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1, then the VLAN IDs will be swapped as shown below.

Figure 2: Configuring VLAN Translation



- ◆ The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.
- ◆ If VLAN translation is set on an interface with this command, and the same interface is also configured as a QinQ access port with the **switchport dot1q-tunnel mode** command, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

## Example

This example configures VLAN translation for Port 1 as described in the Command Usage section above.

```

Console(config)#vlan database
Console(config-vlan)#vlan 10 media ethernet state active
Console(config-vlan)#vlan 100 media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/1,2
Console(config-if)#switchport allowed vlan add 10 tagged
Console(config-if)#switchport allowed vlan add 100 tagged
Console(config-if)#interface ethernet 1/1
Console(config-if)#switchport vlan-translation 10 100
Console(config-if)#end
Console#show vlan-translation

Interface Old VID New VID
-----
Eth 1/ 1      10    100

```

```
Console#
```

**show vlan-translation** This command displays the configuration settings for VLAN translation.

### Syntax

```
show vlan-translation [egress [interface interface] | ingress  
[interface interface]] interface interface
```

**egress** - Show configuration settings for egress ports.

**ingress** - Show configuration settings for ingress ports.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-28/52)

### Command Mode

Privileged Exec

### Example

```
Console#show vlan-translation  
  
Interface Old VID New VID  
-----  
Eth 1/ 1      10    100  
  
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 101: 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 480). 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*<sup>12</sup> - 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.

12. SNAP frame types are not supported by this switch due to hardware limitations.

## 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)

*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*] [**sort-by-type**]

*group-id* - Group identifier for a protocol group. (Range: 1-2147483647)

**sort-by-type** - Sort display information by frame type and protocol type.

#### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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 IP Subnet 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 IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

**Table 102: IP Subnet VLAN Commands**

Command	Function	Mode
<code>subnet-vlan</code>	Defines the IP Subnet VLANs	GC
<code>show subnet-vlan</code>	Displays IP Subnet VLAN settings	PE

**subnet-vlan** This command configures IP Subnet VLAN assignments. Use the **no** form to remove an IP subnet-to-VLAN assignment.

### Syntax

**subnet-vlan subnet** *ip-address mask* **vlan** *vlan-id* [**priority** *priority*]

**no subnet-vlan subnet** [*ip-address mask* | **all**]

*ip-address* – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

*mask* – This mask identifies the host address bits of the IP subnet.

*vlan-id* – VLAN to which matching IP subnet 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

Priority: 0

### Command Mode

Global Configuration

### Command Usage

- ◆ Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask. The specified VLAN need not be an existing VLAN.
- ◆ When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- ◆ The IP subnet cannot be a broadcast or multicast IP address.
- ◆ When MAC-based, IP subnet-based, or protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

### Example

The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

**show subnet-vlan** This command displays IP Subnet VLAN assignments.

**Command Mode**

Privileged Exec

**Command Usage**

- ◆ Use this command to display subnet-to-VLAN mappings.
- ◆ The last matched entry is used if more than one entry can be matched.

**Example**

The following example displays all configured IP subnet-based VLANs.

```
Console#show subnet-vlan
IP Address      Mask                VLAN ID  Priority
-----
192.168.12.0    255.255.255.128    1        0
192.168.12.128 255.255.255.192    3        0
192.168.12.192 255.255.255.224    4        0
192.168.12.224 255.255.255.240    5        0
192.168.12.240 255.255.255.248    6        0
192.168.12.248 255.255.255.252    7        0
192.168.12.252 255.255.255.254    8        0
192.168.12.254 255.255.255.255    9        0
192.168.12.255 255.255.255.255    10       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 103: MAC Based VLAN Commands**

Command	Function	Mode
mac-vlan	Defines the IP Subnet VLANs	GC
show mac-vlan	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-xxxxxxx-xxxxxxx-xxxxxxx-xxxxxxx

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 104: 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



**Table 104: Voice VLAN Commands** (Continued)

Command	Function	Mode
<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: 1-32 characters)

### 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 681](#) 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.”

## 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 Disabled Disabled OUI                6 NA
Eth 1/ 3 Manual   Enabled OUI                5 100
Eth 1/ 4 Auto      Disabled OUI                6 Not Start
Eth 1/ 5 Disabled Disabled OUI                6 NA
Eth 1/ 6 Disabled Disabled OUI                6 NA
Eth 1/ 7 Disabled Disabled OUI                6 NA
Eth 1/ 8 Disabled Disabled OUI                6 NA
Eth 1/ 9 Disabled Disabled OUI                6 NA
Eth 1/10 Disabled 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#

```





# ERPS Commands

The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings.

This chapter describes commands used to configure ERPS.

**Table 105: ERPS Commands**

Command	Function	Mode
<code>erps</code>	Enables ERPS globally on the switch	GC
<code>erps domain</code>	Creates an ERPS ring and enters ERPS configuration mode	GC
<code>control-vlan</code>	Adds a Control VLAN to an ERPS ring	ERPS
<code>enable</code>	Activates the current ERPS ring	ERPS
<code>guard-timer</code>	Sets the timer to prevent ring nodes from receiving outdated R-APS messages	ERPS
<code>holdoff-timer</code>	Sets the timer to filter out intermittent link faults	ERPS
<code>major-domain</code>	Specifies the ERPS ring used for sending control packets	ERPS
<code>meg-level</code>	Sets the Maintenance Entity Group level for a ring	ERPS
<code>mep-monitor</code>	Specifies the CCM MEPs used to monitor the link on a ring node	ERPS
<code>node-id</code>	Sets the MAC address for a ring node	ERPS
<code>non-erps-dev-protect</code>	Sends non-standard health-check packets when in protection state	ERPS
<code>non-revertive</code>	Enables non-revertive mode, which requires the protection state on the RPL to manually cleared	ERPS
<code>propagate-tc</code>	Enables propagation of topology change messages from a secondary ring to the primary ring	ERPS
<code>raps-def-mac</code>	Sets the switch's MAC address to be used as the node identifier in R-APS messages	ERPS
<code>raps-without-vc</code>	Terminates the R-APS channel at the primary ring to sub-ring interconnection nodes	ERPS
<code>ring-port</code>	Configures a node's connection to the ring through the east or west interface	ERPS
<code>rpl neighbor</code>	Configures a ring node to be the RPL neighbor	ERPS
<code>rpl owner</code>	Configures a ring node to be the RPL owner	ERPS
<code>version</code>	Specifies compatibility with ERPS version 1 or 2	ERPS
<code>wtr-timer</code>	Sets timer to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure	ERPS

Table 105: ERPS Commands (Continued)

Command	Function	Mode
<code>clear erps statistics</code>	Clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages	PE
<code>erps clear</code>	Manually clears protection state which has been invoked by a Forced Switch or Manual Switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode	PE
<code>erps forced-switch</code>	Blocks the specified ring port	PE
<code>erps manual-switch</code>	Blocks the specified ring port, in the absence of a failure or an <code>erps forced-switch</code> command	PE
<code>show erps</code>	Displays status information for all configured rings, or for a specified ring	PE

#### Configuration Guidelines for ERPS

1. Create an ERPS ring: Create a ring using the `erps domain` command. The ring name is used as an index in the G.8032 database.
2. Configure the east and west interfaces: Each node on the ring connects to it through two ring ports. Use the `ring-port` command to configure one port connected to the next node in the ring to the east (or clockwise direction); and then use the `ring-port` command again to configure another port facing west in the ring.
3. Configure the RPL owner: Configure one node in the ring as the Ring Protection Link (RPL) owner using the `rpl owner` command. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL. Under normal operations (Idle state), the RPL is blocked to ensure that a loop cannot form in the ring. If a signal failure brings down any other link in the ring, the RPL will be unblocked (Protection state) to ensure proper connectivity among all ring nodes until the failure is recovered.
4. Configure ERPS timers: Use the `guard-timer` command to set the timer is used to prevent ring nodes from receiving outdated R-APS messages, the `holdoff-timer` command to filter out intermittent link faults, and the `wtr-timer` command to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.
5. Configure the ERPS Control VLAN (CVLAN): Use the `control-vlan` command to create the VLAN used to pass R-APS ring maintenance commands. The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN (prior to configuring the VLAN as a CVLAN). No other ports can be members of this VLAN (once set as a CVLAN). Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

6. Enable ERPS: Before enabling a ring as described in the next step, first use the `erps` command to globally enable ERPS on the switch. If ERPS has not yet been enabled or has been disabled with the `no erps` command, no ERPS rings will work.
7. Enable an ERPS ring: Before an ERPS ring can work, it must be enabled using the `enable` command. When configuration is completed and the ring enabled, R-APS messages will start flowing in the control VLAN, and normal traffic will begin to flow in the data VLANs. To stop a ring, it can be disabled on any node using the `no enable` command.
8. Display ERPS status information: Use the `show erps` command to display general ERPS status information or detailed ERPS status information for a specific ring.

**erps** This command enables ERPS on the switch. Use the **no** form to disable this feature.

### Syntax

**[no] erps**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

ERPS must be enabled globally on the switch before it can be enabled on an ERPS ring using the `enable` command.

### Example

```
Console(config)#erps
Console(config)#
```

### Related Commands

[enable \(525\)](#)

**erps domain** This command creates an ERPS ring and enters ERPS configuration mode for the specified domain. Use the **no** form to delete a ring.

### Syntax

**erps domain** *ring-name* [**id** *ring-id*]

**no erps domain** *ring-name*

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

*ring-id* - ERPS ring identifier used in R-APS messages. (Range: 1-255)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

- ◆ Service Instances within each ring are based on a unique maintenance association for the specific users, distinguished by the ring name, maintenance level, maintenance association's name, and assigned VLAN. Up to 6 ERPS rings can be configured on the switch.
- ◆ R-APS information is carried in an R-APS PDUs. The last octet of the MAC address is designated as the Ring ID (01-19-A7-00-00-[Ring ID]). If use of the default MAC address is disabled with the **no raps-def-mac** command, then the Ring ID configured by the **erps domain** command will be used in R-APS PDUs.

### Example

```
Console(config)#erps domain r&d id 1
Console(config-erps)#
```

**control-vlan** This command specifies a dedicated VLAN used for sending and receiving ERPS protocol messages. Use the **no** form to remove the Control VLAN.

### Syntax

[**no**] **control-vlan** *vlan-id*

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

### Default Setting

None

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN ([vlan, page 480](#)), add the ring ports for the east and west interface as tagged members to this VLAN ([switchport allowed vlan, page 483](#)), and then use the [control-vlan](#) command to add it to the ring.
- ◆ The following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:
  - The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.
  - In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.
  - Also, the ring ports of the Control VLAN must be tagged.
- ◆ Once the ring has been activated with the [enable](#) command, the configuration of the control VLAN cannot be modified. Use the [no enable](#) command to stop the ERPS ring before making any configuration changes to the control VLAN.

### Example

```

Console(config)#vlan database
Console(config-vlan)#vlan 2 name rdc media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#interface ethernet 1/11
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#exit
Console(config)#erps domain rd1
Console(config-erps)#control-vlan 2
Console(config-erps)#

```

**enable** This command activates the current ERPS ring. Use the **no** form to disable the current ring.

### Syntax

**[no] enable**

### Default Setting

Disabled

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Before enabling a ring, the global ERPS function should be enabled with the [erps](#) command, the east and west ring ports configured on each node with the

`ring-port` command, the RPL owner specified with the `rpl owner` command, and the control VLAN configured with the `control-vlan` command.

- ◆ Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

### Example

```
Console(config-erps)#enable
Console(config-erps)#
```

### Related Commands

[erps \(523\)](#)

**guard-timer** This command sets the guard timer to prevent ring nodes from receiving outdated R-APS messages. Use the **no** form to restore the default setting.

### Syntax

**guard-timer** *milliseconds*

*milliseconds* - The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds)

### Default Setting

500 milliseconds

### Command Mode

ERPS Configuration

### Command Usage

The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

### Example

```
Console(config-erps)#guard-timer 300
Console(config-erps)#
```

**holdoff-timer** This command sets the timer to filter out intermittent link faults. Use the **no** form to restore the default setting.

### Syntax

**holdoff-timer** *milliseconds*

*milliseconds* - The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds)

### Default Setting

0 milliseconds

### Command Mode

ERPS Configuration

### Command Usage

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer.

When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

### Example

```
Console(config-erps)#holdoff-timer 300
Console(config-erps)#
```

**major-domain** This command specifies the ERPS ring used for sending control packets. Use the **no** form to remove the current setting.

### Syntax

**major-domain** *name*

**no major-domain**

*name* - Name of the ERPS ring used for sending control packets.  
(Range: 1-32 characters)

### Default Setting

None

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ This switch can support up to six rings. However, ERPS control packets can only be sent on one ring. This command is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets.
- ◆ The Ring Protection Link (RPL) is the west port and can not be configured. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. This command will therefore fail if the east port is already configured (see the [ring-port](#) command).

**Example**

```
Console(config-erps)#major-domain rd0
Console(config-erps)#
```

**meg-level** This command sets the Maintenance Entity Group level for a ring. Use the **no** form to restore the default setting.

**Syntax****meg-level** *level*

*level* - The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7)

**Default Setting**

1

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.
- ◆ If CFM continuity check messages are used to monitor the link status of an ERPS ring node as specified by the [mep-monitor](#) command, then the MEG level set by the **meg-level** command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs. The MEP's primary VLAN must also be the same as that used for the ERPS ring's control VLAN.



### Example

```
Console(config-erps)#meg-level 0
Console(config-erps)#
```

### Related Commands

[ethernet cfm domain \(711\)](#)

[ethernet cfm mep \(716\)](#)

**mep-monitor** This command specifies the CFM MEPs used to monitor the link on a ring node. Use the **no** form to restore the default setting.

### Syntax

**mep-monitor** {**east** | **west**} **mep** *mpid*

**east** - Connects to next ring node to the east.

**west** - Connects to next ring node to the west.

*mpid* - Maintenance end point identifier. (Range: 1-8191)

### Default Setting

None

### Command Mode

ERPS Configuration

### Command Usage

- ◆ If this command is used to monitor the link status of an ERPS node with CFM continuity check messages, then the MEG level set by the [meg-level](#) command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs.
- ◆ To ensure complete monitoring of a ring node, use the **mep-monitor** command to specify the CFM MEPs used to monitor both the east and west ports of the ring node.
- ◆ If CFM determines that a MEP node which has been configured to monitor a ring port with this command has gone down, this information is passed to ERPS, which in turn processes it as a ring node failure. For more information on how ERPS recovers from a node failure, refer to "Ethernet Ring Protection Switching" in the *Web Management Guide*.

### Example

```
Console(config-erps)#mep-monitor east mep 1
Console(config-erps)#
```

**Related Commands**[ethernet cfm domain \(711\)](#)[ethernet cfm mep \(716\)](#)

**node-id** This command sets the MAC address for a ring node. Use the **no** form to restore the default setting.

**Syntax**

**node-id** *mac-address*

*mac-address* – A MAC address unique to the ring node. The MAC address must be specified in the format *xx-xx-xx-xx-xx-xx* or *xxxxxxxxxxxx*.

**Default Setting**

CPU MAC address

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ The ring node identifier is used to identify a node in R-APS messages for both automatic and manual switching recovery operations.

For example, a node that has one ring port in SF condition and detects that the condition has been cleared, will continuously transmit R-APS (NR) messages with its own Node ID as priority information over both ring ports, informing its neighbors that no request is present at this node. When another recovered node holding the link blocked receives this message, it compares the Node ID information with its own. If the received R-APS (NR) message has a higher priority, this unblocks its ring ports. Otherwise, the block remains unchanged.

- ◆ The node identifier may also be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

**Example**

```
Console(config-erps)#node-id 00-12-CF-61-24-2D
Console(config-erps)#
```

**non-erps-dev-protect** This command sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through SF messages. Use the **no** form to disable this feature.

**Syntax**

**[no] non-erps-dev-protect**

## Default Setting

Disabled

## Command Mode

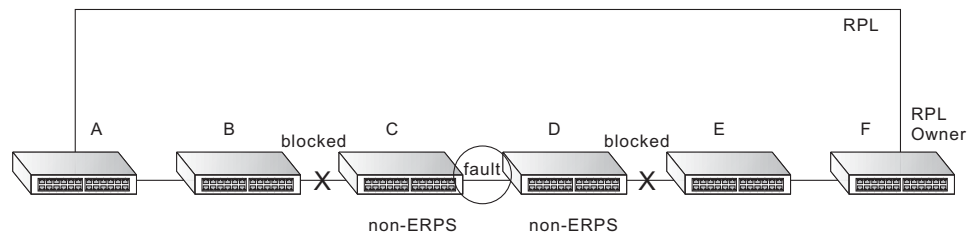
ERPS Configuration

## Command Usage

- ◆ The RPL owner node detects a failed link when it receives R-APS (SF - signal fault) messages from nodes adjacent to the failed link. The owner then enters protection state by unblocking the RPL. However, using this standard recovery procedure may cause a non-ERPS device to become isolated when the ERPS device adjacent to it detects a continuity check message (CCM) loss event and blocks the link between the non-ERPS device and ERPS device.

CCMs are propagated by the Connectivity Fault Management (CFM) protocol as described under [“CFM Commands” on page 705](#). If the standard recovery procedure were used as shown in the following figure, and node E detected CCM loss, it would send an R-APS (SF) message to the RPL owner and block the link to node D, isolating that non-ERPS device.

**Figure 3: Non-ERPS Device Protection**



When non-ERPS device protection is enabled on the ring, the ring ports on the RPL owner node and non-owner nodes will not be blocked when signal loss is detected by CCM loss events.

- ◆ When non-ERPS device protection is enabled on an RPL owner node, it will send non-standard health-check packets to poll the ring health when it enters the protection state. It does not use the normal procedure of waiting to receive an R-APS (NR - no request) message from nodes adjacent to the recovered link. Instead, it waits to see if the non-standard health-check packets loop back. If they do, indicating that the fault has been resolved, the RPL will be blocked.

After blocking the RPL, the owner node will still transmit an R-APS (NR, RB - ring blocked) message. ERPS-compliant nodes receiving this message flush their forwarding database and unblock previously blocked ports. The ring is now returned to Idle state.

## Example

```
Console(config-erps) #non-erps-dev-protect
Console(config-erps) #
```

**non-revertive** This command enables non-revertive mode, which requires the protection state on the RPL to manually cleared. Use the **no** form to restore the default revertive mode.

### Syntax

**[no] non-revertive**

### Default Setting

Disabled

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Revertive behavior allows the switch to automatically return the RPL from Protection state to Idle state through the exchange of protocol messages.

Non-revertive behavior for Protection, Forced Switch, and Manual Switch states are basically the same. Non-revertive behavior requires the [erps clear](#) command to used to return the RPL from Protection state to Idle state.

- ◆ Recovery for Protection Switching – A ring node that has one or more ring ports in an SF (Signal Fail) condition, upon detecting the SF condition cleared, keeps at least one of its ring ports blocked for the traffic channel and for the R-APS channel, until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

A ring node that has one ring port in an SF condition and detects the SF condition cleared, continuously transmits the R-APS (NR – no request) message with its own Node ID as the priority information over both ring ports, informing that no request is present at this ring node and initiates a guard timer. When another recovered ring node (or nodes) holding the link block receives this message, it compares the Node ID information with its own Node ID. If the received R-APS (NR) message has the higher priority, this ring node unblocks its ring ports. Otherwise, the block remains unchanged. As a result, there is only one link with one end blocked.

The ring nodes stop transmitting R-APS (NR) messages when they accept an R-APS (NR, RB – RPL Blocked), or when another higher priority request is received.

- Recovery with Revertive Mode – When all ring links and ring nodes have recovered and no external requests are active, reversion is handled in the following way:
  - a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTR (Wait-to-Restore) timer.
  - b. The WTR timer is cancelled if during the WTR period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.
  - c. When the WTR timer expires, without the presence of any other higher priority request, the RPL Owner Node initiates reversion by blocking its

traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and performing a flush FDB action.

- d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL link that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF (do not flush) indication, all ring nodes flush the FDB.
- Recovery with Non-revertive Mode – In non-revertive operation, the ring does not automatically revert when all ring links and ring nodes have recovered and no external requests are active. Non-revertive operation is handled in the following way:
    - a. The RPL Owner Node does not generate a response on reception of an R-APS (NR) messages.
    - b. When other healthy ring nodes receive the NR (Node ID) message, no action is taken in response to the message.
    - c. When the operator issues the `erps clear` command for non-revertive mode at the RPL Owner Node, the non-revertive operation is cleared, the RPL Owner Node blocks its RPL port, and transmits an R-APS (NR, RB) message in both directions, repeatedly.
    - d. Upon receiving an R-APS (NR, RB) message, any blocking node should unblock its non-failed ring port. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush the FDB.
  - ◆ Recovery for Forced Switching – An `erps forced-switch` command is removed by issuing the `erps clear` command to the same ring node where Forced Switch mode is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

The ring node where the Forced Switch was cleared keeps the ring port blocked for the traffic channel and for the R-APS channel, due to the previous Forced Switch command. This ring port is kept blocked until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

The ring node where the Forced Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing other nodes that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

If the ring node where the Forced Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message over both ring ports.

- Recovery with revertive mode is handled in the following way:
  - a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTB timer.

- b. The WTB timer is cancelled if during the WTB period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.
  - c. When the WTB timer expires, in the absence of any other higher priority request, the RPL Owner Node initiates reversion by blocking the traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes the FDB.
  - d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.
- a. The RPL Owner Node, upon reception of an R-APS(NR) message and in the absence of any other higher priority request does not perform any action.
    - b. Then, after the operator issues the `erps clear` command at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message on both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.
    - c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.
- ◆ Recovery for Manual Switching – An `erps manual-switch` command is removed by issuing the `erps clear` command at the same ring node where the Manual Switch is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

The ring node where the Manual Switch was cleared keeps the ring port blocked for the traffic channel and for the R-APS channel, due to the previous Manual Switch command. This ring port is kept blocked until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

The Ethernet Ring Node where the Manual Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

If the ring node where the Manual Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message on both ring ports.

- Recovery with revertive mode is handled in the following way:
  - a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request, starts the WTB timer and waits for it to expire. While the WTB timer is running, any latent R-APS (MS) message is ignored due to the higher priority of the WTB running signal.
  - b. When the WTB timer expires, it generates the WTB expire signal. The RPL Owner Node, upon reception of this signal, initiates reversion by blocking the traffic channel on the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.
  - c. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all Ethernet Ring Nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.
  
- Recovery with non-revertive mode is handled in the following way:
  - a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request does not perform any action.
  - b. Then, after the operator issues the `erps clear` command at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.
  - c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.

### Example

```
Console(config-erps) #non-revertive
Console(config-erps) #
```

**propagate-tc** This command enables propagation of topology change messages for a secondary ring to the primary ring. Use the **no** form to disable this feature.

### Syntax

**[no] propagate-tc**

### Default Setting

Disabled

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through protection switching.
- ◆ When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

**Example**

```
Console(config-erps) #propagate-tc
Console(config-erps) #
```

**raps-def-mac** This command sets the switch's MAC address to be used as the node identifier in R-APS messages. Use the **no** form to use the node identifier specified in the G8032 standards.

**Syntax**

**[no] raps-def-mac**

**Default Setting**

Enabled

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ When ring nodes running ERPSv1 and ERPSv2 co-exist on the same ring, the Ring ID of each ring node must be configured as "1".
- ◆ If this command is disabled, the following strings are used as the node identifier:
  - ERPSv1: 01-19-A7-00-00-01
  - ERPSv2: 01-19-A7-00-00-[Ring ID]

**Example**

```
Console(config-erps) #raps-def-mac
Console(config-erps) #
```



**raps-without-vc** This command terminates the R-APS channel at the primary ring to sub-ring interconnection nodes. Use the **no** form to restore the default setting.

### Syntax

**[no] raps-without-vc**

### Default Setting

R-APS with Virtual Channel

### Command Mode

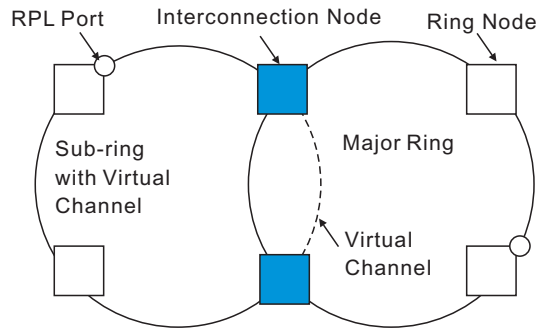
ERPS Configuration

### Command Usage

- ◆ A sub-ring may be attached to a primary ring with or without a virtual channel. A virtual channel is used to connect two interconnection points on the sub-ring, tunneling R-APS control messages across an arbitrary Ethernet network topology. If a virtual channel is not used to cross the intermediate Ethernet network, data in the traffic channel will still flow across the network, but the all R-APS messages will be terminated at the interconnection points.
- ◆ Sub-ring with R-APS Virtual Channel – When using a virtual channel to tunnel R-APS messages between interconnection points on a sub-ring, the R-APS virtual channel may or may not follow the same path as the traffic channel over the network. R-APS messages that are forwarded over the sub-ring's virtual channel are broadcast or multicast over the interconnected network. For this reason the broadcast/multicast domain of the virtual channel should be limited to the necessary links and nodes. For example, the virtual channel could span only the interconnecting rings or sub-rings that are necessary for forwarding R-APS messages of this sub-ring. Care must also be taken to ensure that the local RAPS messages of the sub-ring being transported over the virtual channel into the interconnected network can be uniquely distinguished from those of other interconnected ring R-APS messages. This can be achieved by, for example, by using separate VIDs for the virtual channels of different sub-rings.

Note that the R-APS virtual channel requires a certain amount of bandwidth to forward R-APS messages on the interconnected Ethernet network where a sub-ring is attached. Also note that the protection switching time of the sub-ring may be affected if R-APS messages traverse a long distance over an R-APS virtual channel.

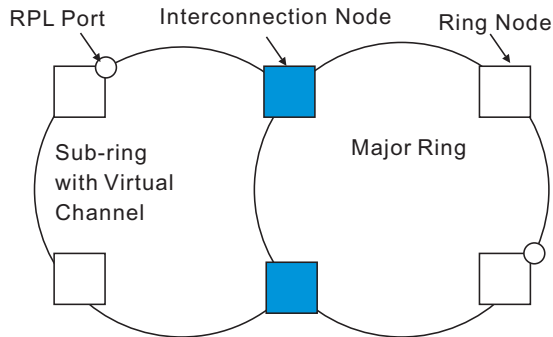
**Figure 4: Sub-ring with Virtual Channel**



- ◆ **Sub-ring without R-APS Virtual Channel** – Under certain circumstances it may not be desirable to use a virtual channel to interconnect the sub-ring over an arbitrary Ethernet network. In this situation, the R-APS messages are terminated on the interconnection points. Since the sub-ring does not provide an R-APS channel nor R-APS virtual channel beyond the interconnection points, R-APS channel blocking is not employed on the normal ring links to avoid channel segmentation. As a result, a failure at any ring link in the sub-ring will cause the R-APS channel of the sub-ring to be segmented, thus preventing R-APS message exchange between some of the sub-ring’s ring nodes.

No R-APS messages are inserted or extracted by other rings or sub-rings at the interconnection nodes where a sub-ring is attached. Hence there is no need for either additional bandwidth or for different VIDs/Ring IDs for the ring interconnection. Furthermore, protection switching time for a sub-ring is independent from the configuration or topology of the interconnected rings. In addition, this option always ensures that an interconnected network forms a tree topology regardless of its interconnection configuration. This means that it is not necessary to take precautions against forming a loop which is potentially composed of a whole interconnected network.

**Figure 5: Sub-ring without Virtual Channel**



**Example**

```
Console(config-erps) #raps-without-vc
Console(config-erps) #
```

**ring-port** This command configures a node's connection to the ring through the east or west interface. Use the **no** form to disassociate a node from the ring.

### Syntax

**ring-port** {**east** | **west**} **interface** *interface*

**east** - Connects to next ring node to the east.

**west** - Connects to next ring node to the west.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### Default Setting

Not associated

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction.
- ◆ Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk.
- ◆ If a port channel (static trunk) is specified as a ring port, it can not be destroyed before it is removed from the domain configuration.
- ◆ A static trunk will be treated as a signal fault, if it contains no member ports or all of its member ports are in signal fault.
- ◆ If a static trunk is configured as a ring port prior to assigning any member ports, spanning tree will be disabled for the first member port assigned to the static trunk.

### Example

```
Console(config-erps)#ring-port east interface ethernet 1/12
Console(config-erps)#
```

**rpl neighbor** This command configures a ring node to be the Ring Protection Link (RPL) neighbor. Use the **no** form to restore the default setting.

#### Syntax

```
rpl neighbor
no rpl
```

#### Default Setting

None (that is, neither owner nor neighbor)

#### Command Mode

ERPS Configuration

#### Command Usage

- ◆ The RPL neighbor node, when configured, is a ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block at the other end by the RPL Owner Node. The RPL neighbor node may participate in blocking or unblocking its end of the RPL, but is not responsible for activating the reversion behavior.
- ◆ Only one RPL owner can be configured on a ring. If the switch is set as the RPL owner for an ERPS domain, the west ring port is set as one end of the RPL. If the switch is set as the RPL neighbor for an ERPS domain, the east ring port is set as the other end of the RPL.
- ◆ The east and west connections to the ring must be specified for all ring nodes using the [ring-port](#) command. When this switch is configured as the RPL neighbor, the east ring port is set as being connected to the RPL.
- ◆ Note that is not mandatory to declare a RPL neighbor.

#### Example

```
Console(config-erps)#rpl neighbor
Console(config-erps)#
```

**rpl owner** This command configures a ring node to be the Ring Protection Link (RPL) owner. Use the **no** form to restore the default setting.

#### Syntax

```
rpl owner
no rpl
```

#### Default Setting

None (that is, neither owner nor neighbor)

## Command Mode

ERPS Configuration

## Command Usage

- ◆ Only one RPL owner can be configured on a ring. The owner blocks traffic on the RPL during Idle state, and unblocks it during Protection state (that is, when a signal fault is detected on the ring or the protection state is enabled with the [erps forced-switch](#) or [erps manual-switch](#) command).
- ◆ The east and west connections to the ring must be specified for all ring nodes using the [ring-port](#) command. When this switch is configured as the RPL owner, the west ring port is automatically set as being connected to the RPL.

## Example

```
Console(config-erps)#rpl owner
Console(config-erps)#
```

**version** This command specifies compatibility with ERPS version 1 or 2.

## Syntax

**version {1 | 2}**

1 - ERPS version 1 based on ITU-T G.8032/Y.1344.

2 - ERPS version 2 based on ITU-T G.8032/Y.1344 Version 2.

## Default Setting

2

## Command Mode

ERPS Configuration

## Command Usage

- ◆ In addition to the basic features provided by version 1, version 2 also supports:
  - Multi-ring/ladder network support
  - Revertive/Non-revertive recovery
  - Forced Switch (FS) and Manual Switch (MS) commands for manually blocking a particular ring port
  - Flush FDB (forwarding database) logic which reduces amount of flush FDB operations in the ring
  - Support of multiple ERP instances on a single ring
- ◆ Version 2 is backward compatible with Version 1. If version 2 is specified, the inputs and commands are forwarded transparently. If set to version 1, MS and FS operator commands are filtered, and the switch set to revertive mode.

- ◆ The version number is automatically set to “1” when a ring node, supporting only the functionalities of G.8032v1, exists on the same ring with other nodes that support G.8032v2.
- ◆ When ring nodes running G.8032v1 and G.8032v2 co-exist on a ring, the ring ID of each node is configured as “1”.
- ◆ In version 1, the MAC address 01-19-A7-00-00-01 is used for the node identifier. The `raps-def-mac` command has no effect.

### Example

```
Console(config-erps)#version 1
Console(config-erps)#
```

**wtr-timer** This command sets the wait-to-restore timer which is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. Use the **no** form to restore the default setting.

### Syntax

**wtr-timer** *minutes*

*minutes* - The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes)

### Default Setting

5 minutes

### Command Mode

ERPS Configuration

### Command Usage

If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

### Example

```
Console(config-erps)#wtr-timer 10
Console(config-erps)#
```

**clear erps statistics** This command clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages.

### Syntax

**clear erps statistics** [**domain** *ring-name*]

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

### Command Mode

Privileged Exec

### Example

```
Console#clear erps statistics domain r&d
Console#
```

**erps clear** This command manually clears the protection state which has been invoked by a forced switch or manual switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode.

### Syntax

**erps clear domain** *ring-name*

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

### Command Mode

Privileged Exec

### Command Usage

- ◆ Two steps are required to make a ring operating in non-revertive mode return to Idle state from forced switch or manual switch state:
  1. Issue an **erps clear** command to remove the forced switch command on the node where a local forced switch command is active.
  2. Issue an **erps clear** command on the RPL owner node to trigger the reversion.
- ◆ The **erps clear** command will also stop the WTR and WTB delay timers and reset their values.
- ◆ More detailed information about using this command for non-revertive mode is included under the Command Usage section for the [non-revertive](#) command.

**Example**

```
Console#erps clear domain r&d
Console#
```

**erps forced-switch** This command blocks the specified ring port.

**Syntax**

**erps forced-switch** [**domain** *ring-name*] {**east** | **west**}

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

**east** - East ring port.

**west** - West ring port.

**Command Mode**

Privileged Exec

**Command Usage**

- ◆ A ring with no pending request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the **erps forced-switch** command triggers protection switching as follows:
  - a. The ring node where a forced switch command was issued blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.
  - b. The ring node where the forced switch command was issued transmits R-APS messages indicating FS over both ring ports. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command (see [Table 106 on page 545](#)). The R-APS (FS) message informs other ring nodes of the FS command and that the traffic channel is blocked on one ring port.
  - c. A ring node accepting an R-APS (FS) message, without any local higher priority requests unblocks any blocked ring port. This action subsequently unblocks the traffic channel over the RPL.
  - d. The ring node accepting an R-APS (FS) message, without any local higher priority requests stops transmission of R-APS messages.
  - e. The ring node receiving an R-APS (FS) message flushes its FDB.
- ◆ Protection switching on a forced switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on the following rules apply regarding processing of further forced switch commands:



While an existing forced switch request is present in a ring, any new forced switch request is accepted, except on a ring node having a prior local forced switch request. The ring nodes where further forced switch commands are issued block the traffic channel and R-APS channel on the ring port at which the forced switch was issued. The ring node where the forced switch command was issued transmits an R-APS message over both ring ports indicating FS. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command. As such, two or more forced switches are allowed in the ring, which may inadvertently cause the segmentation of an ring. It is the responsibility of the operator to prevent this effect if it is undesirable.

Ring protection requests, commands and R-APS signals have the priorities as specified in the following table.

**Table 106: ERPS Request/State Priority**

Request / State and Status	Type	Priority
Clear	local	highest
FS	local	
R-APS (FS)	remote	
local SF*	local	
local clear SF	local	
R-APS (SF)	remote	
R-APS (MS)	remote	
MS	local	
WTR Expires	local	
WTR Running	local	
WTB Expires	local	
WTB Running	local	
R-APS (NR, RB)	remote	
R-APS (NR)	remote	lowest

\* If an Ethernet Ring Node is in the Forced Switch state, local SF is ignored.

- ◆ Recovery for forced switching under revertive and non-revertive mode is described under the Command Usage section for the [non-revertive](#) command.
- ◆ When a ring is under an FS condition, and the node at which an FS command was issued is removed or fails, the ring remains in FS state because the FS command can only be cleared at node where the FS command was issued. This results in an unrecoverable FS condition.

When performing a maintenance procedure (e.g., replacing, upgrading) on a ring node (or a ring link), it is recommended that FS commands be issued at the two adjacent ring nodes instead of directly issuing a FS command at the ring

node under maintenance in order to avoid falling into the above mentioned unrecoverable situation.

### Example

```
Console#erps forced-switch domain r&d west
Console#
```

**erps manual-switch** This command blocks the specified ring port, in the absence of a failure or an **erps forced-switch** command.

### Syntax

**erps manual-switch** [**domain** *ring-name*] {**east** | **west**}

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

**east** - East ring port.

**west** - West ring port.

### Command Mode

Privileged Exec

### Command Usage

- ◆ A ring with no request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the **erps manual-switch** command triggers protection switching as follows:
  - a. If no other higher priority commands exist, the ring node, where a manual switch command was issued, blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.
  - b. If no other higher priority commands exist, the ring node where the manual switch command was issued transmits R-APS messages over both ring ports indicating MS. R-APS (MS) message are continuously transmitted by this ring node while the local MS command is the ring node's highest priority command (see [Table 106 on page 545](#)). The R-APS (MS) message informs other ring nodes of the MS command and that the traffic channel is blocked on one ring port.
  - c. If no other higher priority commands exist and assuming the ring node was in Idle state before the manual switch command was issued, the ring node flushes its local FDB.
  - d. A ring node accepting an R-APS (MS) message, without any local higher priority requests unblocks any blocked ring port which does not have an SF condition. This action subsequently unblocks the traffic channel over the RPL.

- e. A ring node accepting an R-APS (MS) message, without any local higher priority requests stops transmitting R-APS messages.
  - f. A ring node receiving an R-APS (MS) message flushes its FDB.
- ◆ Protection switching on a manual switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on, the following rules apply regarding processing of further manual switch commands:
    - a. While an existing manual switch request is present in the ring, any new manual switch request is rejected. The request is rejected at the ring node where the new request is issued and a notification is generated to inform the operator that the new MS request was not accepted.
    - b. A ring node with a local manual switch command which receives an R-APS (MS) message with a different Node ID clears its manual switch request and starts transmitting R-APS (NR) messages. The ring node keeps the ring port blocked due to the previous manual switch command.
    - c. An ring node with a local manual switch command that receives an R-APS message or a local request of higher priority than R-APS (MS) clear its manual switch request. The ring node then processes the new higher priority request.
  - ◆ Recovery for manual switching under revertive and non-revertive mode is described under the Command Usage section for the [non-revertive](#) command.

### Example

```
Console#erps manual-switch domain r&d west
Console#
```

**show erps** This command displays status information for all configured rings, or for a specified ring

### Syntax

**show erps** [**domain** *ring-name*] [**statistics**]

**domain** - Keyword to display ERPS ring configuration settings.

*ring-name* - Name of a specific ERPS ring. (Range: 1-32 characters)

**statistics** - Keyword to display ERPS ring statistics.

### Command Mode

Privileged Exec

**Example**

This example displays a summary of all the ERPS rings configured on the switch.

```

Console#show erps
ERPS Status           : Enabled
Number of ERPS Domains : 1

Domain      ID  Enabled Ver  MEL  Ctrl VLAN State      Type      Revertive
-----
r&d        1  Yes    2    1    1  Idle      RPL Owner  Yes

          W/E  Interface Port State  Local SF  Local FS  Local MS  MEP  RPL
          ---  ---
          West Eth 1/ 1  Blocking  No    No    No    No    Yes
          East Eth 1/ 3  Forwarding No    No    No    No    No

```

Console#

**Table 107: show erps - summary display description**

Field	Description
<i>Node Information</i>	
ERPS Status	Shows whether ERPS is enabled on the switch.
Number of ERPS Domains	Shows the number of ERPS rings configured on the switch.
Domain	Displays the name of each ring followed by a brief list of status information
ID	ERPS ring identifier used in R-APS messages.
Enabled	Shows if the specified ring is enabled.
Ver	Shows the ERPS version.
MEL	The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
Ctrl VLAN	Shows the Control VLAN ID.
State	Shows the following ERPS states: Init – The ERPS ring has started but has not yet determined the status of the ring. Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs. Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.
Type	Shows ERPS node type as None, RPL Owner or RPL Neighbor.
Revertive	Shows if revertive or non-revertive recovery is selected.
<i>Interface Information</i>	
W/E	Shows information on the west and east ring port for this node.
Interface	The port or trunk which is configured as a ring port.

**Table 107: show erps - summary display description** (Continued)

Field	Description
Port State	The operational state:  Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.  Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed.  Unknown – The interface is not in a known state (includes the domain being disabled).
Local SF	A signal fault generated on a link to the local node.
Local FS	Shows if a forced switch command was issued on this interface.
Local MS	Shows if a manual switch command was issued on this interface.
MEP	The CFM MEP used to monitor the status on this link.
RPL	Shows if this node is connected to the RPL.

This example displays detailed information for the specified ERPS ring.

```

Console#show erps domain rd1
Domain      ID  Enabled Ver  MEL  Ctrl  VLAN  State      Type      Revertive
-----
r&d        1  Yes     2    1     1    Idle      RPL Owner  Yes

          Major Domain Node ID          R-APS With VC
          -----
                   00-E0-0C-00-00-FD Yes

R-APS Def MAC Propagate TC Non-ERPS Device Protect
-----
Yes           No           No

Holdoff  Guard  WTB    WTR    WTB Expire WTR Expire
-----
    0 ms  500 ms 5500 ms  5 min

W/E  Interface Port State Local SF Local FS Local MS MEP  RPL
-----
West Eth 1/ 1 Blocking No      No      No      Yes
East Eth 1/ 3 Forwarding No      No      No      No

```

Console#

[Table 107 on page 548](#) describes most of the parameters shown by **show erps domain** command. The following table includes the remaining parameters.

**Table 108: show erps domain - detailed display description**

Field	Description
Major Domain	Name of the ERPS major domain.
Node ID	A MAC address unique to this ring node.

**Table 108: show erps domain - detailed display description** (Continued)

Field	Description
R-APS with VC	The R-APS Virtual Channel is the R-APS channel connection used to tunnel R-APS messages between two interconnection nodes of a sub-ring in another Ethernet ring or network.
R-APS Def MAC	Indicates if the switch's MAC address is used to identify the node in R-APS messages.
Propagate TC	Shows if the ring is configured to propagate topology change notification messages.
Non-ERPS Device Protect	Shows if the RPL owner node is configured to send non-standard health-check packets when it enters protection state without any link down event having been detected through SF messages
Holdoff	The hold-off timer interval used to filter out intermittent link faults.
Guard	The guard timer interval used to prevent ring nodes from receiving outdated R-APS messages.
WTB	The wait-to-block timer interval used to delay reversion after a Forced Switch or Manual Switch has been cleared.
WTR	The wait-to-restore timer interval used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.
WTB Expire	The time before the wait-to-block timer expires.
WTR Expire	The time before the wait-to-restore timer expires.

This example displays statistics for all configured ERPS rings.

```

Console#show erps statistics
ERPS statistics for domain r&d :
Interface   Local SF   Local Clear SF
-----
(W) Eth 1/ 1 0
            SF      NR      NR-RB    FS      MS
-----
Sent        0        62      948      0        0
Received    0        0        0        0        0
Ignored     0        0        0        0        0
            EVENT   HEALTH
-----
Sent        0        0
Received    0        0
Ignored     0        0

Interface   Local SF   Local Clear SF
-----
(E) Eth 1/ 3 0
            SF      NR      NR-RB    FS      MS
-----
Sent        0        62      948      0        0
Received    0        0        0        0        0
Ignored     0        0        0        0        0
            EVENT   HEALTH
-----
Sent        0        0
Received    0        0
Ignored     0        0
Console#
    
```

**Table 109: show erps statistics - detailed display description**

<b>Field</b>	<b>Description</b>
Interface	The direction, and port or trunk which is configured as a ring port.
Local SF	A signal fault generated on a link to the local node.
Local Clear SF	The number of times a clear command was issued to terminate protection state entered through a forced switch or manual switch
SF	The number of signal fault messages
NR	The number of no request messages
NR-RB	The number no request - RPL blocked messages
FS	The number of forced switch messages
MS	The number of manual switch messages
EVENT	Any request/state message, excluding FS, SF, MS, and NR
HEALTH	The number of non-standard health-check messages





## 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 110: 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 111: 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, Port Channel)

### 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 \(555\)](#)  
[show queue mode \(557\)](#)

**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, Port Channel)

### 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 554](#)).
- ◆ 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 \(554\)](#)

[show queue weight \(557\)](#)

**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 \(388\)](#)

**show queue mode** This command shows the current queue mode.

### 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.

### 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 112: 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 113: Default Mapping of CoS/CFI Values to Queue/CFI

CoS	CFI	0	1
0		(2,0)	(2,0)
1		(0,0)	(0,0)
2		(1,0)	(1,0)
3		(3,0)	(3,0)
4		(4,0)	(4,0)
5		(5,0)	(5,0)
6		(6,0)	(6,0)
7		(7,0)	(7,0)

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- ◆ The default mapping of CoS/CFI to Queue/CFI values shown in [Table 113](#) 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 114: Default Mapping of DSCP/CFI Values to Queue**

	ingress- dscp1	0	1	2	3	4	5	6	7	8	9
ingress- dscp10		0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1		1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2		2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3,0	3,1
3		3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4,0	4,3
4		5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5		6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7,0	7,3
6		7,0	7,1	7,0	7,3						

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, ingress-dscp = ingress-dscp10 \* 10 + ingress-dscp1)); and the corresponding dscp is shown at the intersecting cell in the table.

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**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, Port Channel)

### 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 556](#)) 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 556](#)) 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: 1-26/28/52)

### 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: 1-26/28/52)

#### 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, ingress-dscp = ingress-dscp10 \* 10 + 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
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: 1-26/28/52)

**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 115: Quality of Service Commands**

Command	Function	Mode
<code>class-map</code>	Creates a class map for a type of traffic	GC
<code>description</code>	Specifies the description of a class map	CM
<code>match</code>	Defines the criteria used to classify traffic	CM
<code>rename</code>	Redefines the name of a class map	CM
<code>policy-map</code>	Creates a policy map for multiple interfaces	GC
<code>description</code>	Specifies the description of a policy map	PM
<code>class</code>	Defines a traffic classification for the policy to act on	PM
<code>rename</code>	Redefines the name of a policy map	PM
<code>police rate</code>	Defines an enforcer for classified traffic based on the metered flow rate	PM-C
<code>set cos</code>	Services IP traffic by setting a class of service value for matching packets for internal processing	PM-C
<code>set ip dscp</code>	Services IP traffic by setting a IP DSCP value for matching packets for internal processing	PM-C
<code>service-policy</code>	Applies a policy map defined by the <code>policy-map</code> command to a particular interface	IC
<code>show class-map</code>	Displays the QoS class maps which define matching criteria used for classifying traffic	PE
<code>show policy-map</code>	Displays the QoS policy maps which define classification criteria for ingress or egress traffic, and may include policers for bandwidth limitations	PE
<code>show policy-map interface</code>	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` or `set ip dscp` command to modify the per-hop behavior, the class of service value in the VLAN tag, or the priority bits in the IP header (IP DSCP value) 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
```

*class-map-name* - Name of the class map. (Range: 1-32 characters)

#### 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 570](#)). The policy map is then bound by a service policy to an interface ([page 574](#)). 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 ip dscp 3
Console(config-cmap)#
```

### Related Commands

[show class-map \(574\)](#)

**description** This command specifies the description of a class map or policy map.

### Syntax

**description** *string*

*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 | source-port interface |
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)

*interface*

*unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

*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 570](#)) 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.)
  - **set ip dscp** command sets the IP DSCP value in matching packets. (This modifies packet priority in the IP header.)
  - **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 new-dscp**

*new-dscp* - New 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 or egress side of a particular interface. Use the **no** form to remove this mapping.

### Syntax

**[no] service-policy {input | output} 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, Port Channel)

### Command Usage

- ◆ Only one policy map can be assigned to an interface.
- ◆ 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.

### 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: 1-26/28/52)

#### 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.

**Table 116: 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.
MVR for IPv4	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic
MVR for IPv6	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic

## IGMP Snooping

This section describes commands used to configure IGMP snooping on the switch.

**Table 117: IGMP Snooping Commands**

Command	Function	Mode
<code>ip igmp snooping</code>	Enables IGMP snooping	GC
<code>ip igmp snooping priority</code>	Assigns a priority to all multicast traffic	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

**Table 117: IGMP Snooping Commands** (Continued)

Command	Function	Mode
<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
<code>ip igmp snooping vlan version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping vlan version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>clear ip igmp snooping groups dynamic</code>	Clears multicast group information dynamically learned through IGMP snooping	PE
<code>clear ip igmp snooping statistics</code>	Clears IGMP snooping statistics	PE

**Table 117: IGMP Snooping Commands** (Continued)

Command	Function	Mode
<code>show ip igmp snooping</code>	Shows the IGMP snooping, proxy, and query configuration	PE
<code>show ip igmp snooping group</code>	Shows known multicast group, source, and host port mapping	PE
<code>show ip igmp snooping mrouter</code>	Shows multicast router ports	PE
<code>show ip igmp snooping 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 priority** This command assigns a priority to all multicast traffic. Use the **no** form to restore the default setting.

#### Syntax

**ip igmp snooping priority** *priority*

**no ip igmp snooping priority**

*priority* - The CoS priority assigned to all multicast traffic. (Range: 0-7, where 7 is the highest priority)

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Command Usage

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

#### Example

```
Console(config)#ip igmp snooping priority 6
Console(config)#
```

#### Related Commands

[show ip igmp snooping \(596\)](#)

**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

- ◆ IGMP snooping querier is not supported for IGMPv3 snooping (see [ip igmp snooping version](#)).
- ◆ 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 580](#)).

### 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 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

**ip igmp snooping [vlan *vlan-id*] version-exclusive**

**no ip igmp snooping 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 580](#)).

### 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 580](#)).

#### 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

**[no] ip igmp snooping vlan *vlan-id* proxy-address source-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 581](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 580](#)).

### 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 581), or as a proxy host when IGMP snooping proxy reporting is enabled (page 580).

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 224.0.0.12 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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 | 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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)
		Eth 1/ 2(M)			0 (H)

```
Console#
```

**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*]}

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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 118: 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 119: 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.

**Table 119: show ip igmp snooping statistics output - display description**

Field	Description
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 120: 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.
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.



**Table 120: show ip igmp snooping statistics vlan query - display description**

Field	Description
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 121: 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 122: 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 authentication</code>	Enables RADIUS authentication for IGMP JOIN requests.	IC
<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>ip multicast-data-drop</code>	Drops all multicast data packets	IC
<code>show ip igmp authentication</code>	Displays IGMP authentication settings for interfaces	PE
<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

Table 122: IGMP Filtering and Throttling Commands (Continued)

Command	Function	Mode
<code>show ip igmp throttle interface</code>	Displays the IGMP throttling setting for interfaces	PE
<code>show ip multicast-data-drop</code>	Shows if the interface is configured to drop multicast data packets	PE

**ip igmp filter** (Global Configuration) This command globally enables IGMP filtering and throttling on the switch. Use the **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.
- ◆ The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

### 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. Use the **no** form to delete a profile number.

#### 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 authentication** This command enables IGMP authentication on the specified interface. When enabled and an IGMP JOIN request is received, an authentication request is sent to a configured RADIUS server. Use the **no** form to disable IGMP authentication.

### Syntax

**[no] ip igmp authentication**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ If IGMP authentication is enabled on an interface, and a join report is received on the interface, the switch will send an access request to the RADIUS server to perform authentication.
- ◆ Only when the RADIUS server responds with an authentication success message will the switch learn the group report. Once the group is learned, the switch will not send an access request to the RADIUS server when receiving the same report again within a one (1) day period.
- ◆ If the RADIUS server responds that authentication failed or the timer expires, the report will be dropped and the group will not be learned. The entry (host MAC, port number, VLAN ID, and group IP) will be put in the “authentication failed list”.
- ◆ The “authentication failed list” is valid for the period of the interval defined by the command `ip igmp snooping vlan query-interval`. When receiving the same report during this interval, the switch will not send the access request to the RADIUS server.
- ◆ If the interface leaves the group and subsequently rejoins the same group, the join report needs to again be authenticated.
- ◆ When receiving an IGMP v3 report message, the switch will send the access request to the RADIUS server only when the record type is either IS\_EX or TO\_EX, and the source list is empty. Other types of packets will not initiate RADIUS authentication.

IS\_EX (MODE\_IS\_EXCLUDE) - Indicates that the interface’s filter mode is EXCLUDE for the specified multicast address. The Source Address fields in this Group Record contain the interface’s source list for the specified multicast address, if not empty.

TO\_EX (CHANGE\_TO\_EXCLUDE\_MODE) - Indicates that the interface has changed to EXCLUDE filter mode for the specified multicast address. The Source Address fields in this Group Record contain the interface’s new source list for the specified multicast address, if not empty.

- ◆ When a report is received for the first time and is being authenticated, whether authentication succeeds or fails, the report will still be sent to the multicast-router port.
- ◆ The following table shows the RADIUS server Attribute Value Pairs used for authentication:

**Table 123: IGMP Authentication RADIUS Attribute Value Pairs**

Attribute Name	AVP Type	Entry
USER_NAME	1	User MAC address
USER_PASSWORD	2	User MAC address
NAS_IP_ADDRESS	4	Switch IP address

Table 123: IGMP Authentication RADIUS Attribute Value Pairs

Attribute Name	AVP Type	Entry
NAS_PORT	5	User Port Number
FRAMED_IP_ADDRESS	8	Multicast Group ID

**Example**

This example shows how to enable IGMP Authentication on all of the switch's Ethernet interfaces.

```
Console(config)#interface ethernet 1/1-28
Console(config-if)#ip igmp authentication
Console#
```

**Related Commands**

[show ip igmp authentication](#)

**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**

**[no] ip igmp filter** *profile-number*

*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: 1-1024)

#### Default Setting

1024

#### 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**

### 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)#
```

**ip multicast-data-drop** This command drops all 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 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 igmp authentication

This command displays the interface settings for IGMP authentication.

### Syntax

**show ip igmp authentication interface** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Using this command without specifying an interface displays information for all interfaces.

### Example

```
Console#show ip igmp authentication
Ethernet 1/1: Enabled
Ethernet 1/2: Enabled
Ethernet 1/3: Enabled
:
Ethernet 1/27: Enabled
Ethernet 1/28: Enabled
Other ports/port channels are Disable
Console#
```

**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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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
IGMP Profile 50
```

```
Console#show ip igmp profile 19
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 query-drop** This command shows if the specified interface is configured to drop IGMP query packets.

### Syntax

**show ip igmp throttle interface** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Using this command without specifying an interface displays information for all interfaces.

### 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#
```

**show ip multicast-data-drop** This command shows if the specified interface is configured to drop multicast data packets.

### Syntax

**show ip igmp throttle interface** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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#
```

## 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 124: 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 MLD snooping 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 124: 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 groups	PE
<code>show ipv6 mld snooping group source-list</code>	Displays the learned groups and corresponding source list	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 all-zeros IP source address when forwarding any summarized reports upstream. For this reason, IGMP membership reports received by the snooping switch must not be rejected because the source IP address is set to 0.0.0.0.

### 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 seconds 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 MLD snooping 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 615](#)).

#### Example

```
Console(config)#ipv6 mld snooping unsolicited-report-interval 5  
Console(config)#
```

**ipv6 mld snooping version** This command configures the MLD snooping version. Use the **no** form to restore the default.

#### 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

**ipv6 mld snooping vlan** *vlan-id* **immediate-leave** [**by-host-ip**]

**no ipv6 mld 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 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.
- ◆ If the “by-host-ip” option is used, the router/querier will not send out a group-specific query when an MLD 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.

### Example

The following shows how to enable MLD immediate leave.

```
Console(config)#ipv6 mld snooping immediate-leave
Console(config)#
```

**ipv6 mld snooping** This command statically configures an IPv6 multicast router port. Use the **no** form  
**vlan mrouter** 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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  
vlan static** This command adds a port to an IPv6 multicast group. Use the **no** form to remove 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)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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**

### 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#

```

**show ipv6 mld snooping group source-list** This command shows known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

### Syntax

**show ipv6 mld snooping group source-list** [*ipv6-address* | **vlan** *vlan-id*]

*ipv6-address* - An IPv6 address of a multicast group. (Format: X:X:X::X)

*vlan-id* - VLAN ID (1-4094)

### Command Mode

Privileged Exec

### Example

The following shows MLD Snooping group mapping information:

```
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 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*}

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**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 125: 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.

**Table 125: show ipv6 mld snooping statistics input - display description**

Field	Description
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 126: 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 127: 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:          :                               Report & Leave:  :
  Transmit        :                               Transmit        :
    General       : 6                               Report          : 0
    Group Specific: 0                               Leave           : 0
Recieved         :                               Recieved        :
  General         : 0                               Report          : 4
  Group Specific: 0                               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:          :                               Report & Leave:  :
  Other Querier   : None                               Host Addr       : None
                                                    Unsolicit Expire: 0 sec

  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        :                               Transmit        :
    General       : 7                               Report          : 0
    Group Specific: 0                               Leave           : 0
Recieved         :                               Recieved        :
  General         : 0                               Report          : 4
  Group Specific: 0                               Leave           : 0
                                                    join Success    : 0
                                                    Filter Drop     : 0
                                                    Source Port Drop: 0
                                                    Others Drop     : 0

Console#

```

**Table 128: 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 &amp; Leave</i>	
<i>Transmit</i>	
Report	The number of MLD membership reports sent from this interface.
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 &amp; 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 129: 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
<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>ipv6 multicast-data-drop</code>	Enable multicast data guard mode on a port interface	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. Use the **no** form to delete a profile number.

### 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-ml-d-profile)#range ff01::0101 ff01::0202
Console(config-ml-d-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

**[no] ipv6 mld filter** *profile-number*

*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)

### 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)#
```

**ipv6 multicast-data-drop** Use this command to enable multicast data guard mode on a port interface. Use the no form of the command to disable multicast data guard.

### Syntax

**[no] ipv6 multicast-data-drop**

### Default Setting

Disabled

### Command Mode

Interface Configuration

### Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#ipv6 multicast-data-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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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#
```

## MVR for IPv4

This section describes commands used to configure Multicast VLAN Registration for IPv4 (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

**Table 130: Multicast VLAN Registration for IPv4 Commands**

Command	Function	Mode
<code>mvr</code>	Globally enables MVR	GC
<code>mvr associated-profile</code>	Binds the MVR group addresses specified in a profile to an MVR domain	GC
<code>mvr domain</code>	Enables MVR for a specific domain	GC
<code>mvr priority</code>	Assigns a priority to all multicast traffic in the MVR VLAN	GC
<code>mvr profile</code>	Maps a range of MVR group addresses to a profile	GC
<code>mvr proxy-query-interval</code>	Configures the interval at which the receiver port sends out general queries.	GC
<code>mvr proxy-switching</code>	Enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled	GC
<code>mvr robustness-value</code>	Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries	GC
<code>mvr source-port-mode dynamic</code>	Configures the switch to only forward multicast streams which the source port has dynamically joined	GC
<code>mvr upstream-source-ip</code>	Configures the source IP address assigned to all control packets sent upstream	GC
<code>mvr vlan</code>	Specifies the VLAN through which MVR multicast data is received	GC
<code>mvr immediate-leave</code>	Enables immediate leave capability	IC
<code>mvr type</code>	Configures an interface as an MVR receiver or source port	IC
<code>mvr vlan group</code>	Statically binds a multicast group to a port	IC
<code>clear mvr groups dynamic</code>	Clears multicast group information dynamically learned through MVR	PE
<code>clear mvr statistics</code>	Clears MVR statistics	PE
<code>show mvr</code>	Shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address	PE
<code>show mvr associated-profile</code>	Shows the profiles bound the specified domain	PE



**Table 130: Multicast VLAN Registration for IPv4 Commands** (Continued)

Command	Function	Mode
<code>show mvr interface</code>	Shows MVR settings for interfaces attached to the MVR VLAN	PE
<code>show mvr members</code>	Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address	PE
<code>show mvr profile</code>	Shows all configured MVR profiles	PE
<code>show mvr statistics</code>	Shows MVR protocol statistics for the specified interface	PE

**mvr** This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the **no** form of this command to globally disable MVR.

### Syntax

**[no] mvr**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the `mvr vlan group` command.

### Example

The following example enables MVR globally.

```
Console(config)#mvr
Console(config)#
```

**mvr associated-profile** This command binds the MVR group addresses specified in a profile to an MVR domain. Use the **no** form of this command to remove the binding.

### Syntax

**[no] mvr domain *domain-id* associated-profile *profile-name***

*domain-id* - An independent multicast domain. (Range: 1-5)

*profile-name* - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Example

The following an MVR group address profile to domain 1:

```
Console(config)#mvr domain 1 associated-profile rd
Console(config)#
```

### Related Commands

[mvr profile \(643\)](#)

**mvr domain** This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the **no** form of this command to disable MVR for a domain.

### Syntax

```
[no] mvr domain domain-id
```

*domain-id* - An independent multicast domain. (Range: 1-5)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the [mvr vlan group](#) command.

### Example

The following example enables MVR for domain 1:

```
Console(config)#mvr domain 1
Console(config)#
```

**mvr priority** This command assigns a priority to all multicast traffic in the MVR VLAN. Use the **no** form of this command to restore the default setting.

### Syntax

**mvr priority** *priority*

**no mvr priority**

*priority* - The CoS priority assigned to all multicast traffic forwarded into the MVR VLAN. (Range: 0-7, where 7 is the highest priority)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

### Example

```
Console(config)#mvr priority 6
Console(config)#
```

### Related Commands

[show mvr](#)

**mvr profile** This command maps a range of MVR group addresses to a profile. Use the **no** form of this command to remove the profile.

### Syntax

**mvr profile** *profile-name start-ip-address end-ip-address*

**no mvr profile** *profile-name*

*profile-name* - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

*start-ip-address* - Starting IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

*end-ip-address* - Ending IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

### Default Setting

No profiles are defined

### Command Mode

Global Configuration

### Command Usage

- ◆ Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

### Example

The following example maps a range of MVR group addresses to a profile:

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10  
Console(config)#
```

**mvr proxy-query-interval** This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

### Syntax

**mvr proxy-query-interval** *interval*

**no mvr proxy-query-interval**

*interval* - The interval at which the receiver port sends out general queries.  
(Range: 2-31744 seconds)

### Default Setting

125 seconds

### Command Mode

Global Configuration

### Command Usage

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the **mvr proxy-switching** command.

### Example

This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr proxy-query-interval 250  
Console(config)#
```

**mvr proxy-switching** This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the **no** form to disable this function.

### Syntax

**[no] mvr proxy-switching**

### Default Setting

Enabled

### Command Mode

Global Configuration

### Command Usage

- ◆ When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- ◆ Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- ◆ When the source port receives report and leave messages, it only forwards them to other source ports.
- ◆ When receiver ports receive any query messages, they are dropped.
- ◆ When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- ◆ When MVR proxy switching is disabled:
  - Any membership reports received from receiver/source ports are forwarded to all source ports.
  - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
  - When a receiver port receives a query message, it will be dropped.

### Example

The following example enable MVR proxy switching.

```
Console(config)#mvr proxy-switching  
Console(config)#
```

### Related Commands

[mvr robustness-value \(646\)](#)

**mvr robustness-value** This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the **no** form to restore the default setting.

### Syntax

**mvr robustness-value** *value*

**no mvr robustness-value**

*value* - The robustness used for all interfaces. (Range: 1-255)

### Default Setting

2

### Command Mode

Global Configuration

### Command Usage

- ◆ This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- ◆ This command only takes effect when MVR proxy switching is enabled.

### Example

```
Console(config)#mvr robustness-value 5  
Console(config)#
```

### Related Commands

[mvr proxy-switching \(645\)](#)

**mvr source-port-mode dynamic** This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

### Syntax

**[no] mvr source-port-mode dynamic**

### Default Setting

Forwards all multicast streams which have been specified in a profile and bound to a domain.

### Command Mode

Global Configuration

### Command Usage

- ◆ By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- ◆ When the **mvr source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

### Example

```
Console(config)#mvr source-port-mode dynamic
Console(config)#
```

**mvr upstream-source-ip** This command configures the source IP address assigned to all MVR control packets sent upstream on all domains or on a specified domain. Use the **no** form to restore the default setting.

### Syntax

**mvr [domain *domain-id*] upstream-source-ip *source-ip-address***

**no mvr [domain *domain-id*] upstream-source-ip**

*domain-id* - An independent multicast domain. (Range: 1-5)

*source-ip-address* - The source IPv4 address assigned to all MVR control packets sent upstream.

### Default Setting

All MVR reports sent upstream use a null source IP address

## Command Mode

Global Configuration

## Example

```
Console(config)#mvr domain 1 upstream-source-ip 192.168.0.3  
Console(config)#
```

**mvr vlan** This command specifies the VLAN through which MVR multicast data is received. Use the **no** form of this command to restore the default MVR VLAN.

## Syntax

**mvr domain** *domain-id* **vlan** *vlan-id*

**no mvr domain** *domain-id* **vlan**

*domain-id* - An independent multicast domain. (Range: 1-5)

*vlan-id* - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

## Default Setting

VLAN 1

## Command Mode

Global Configuration

## Command Usage

- ◆ This command specifies the VLAN through which MVR multicast data is received. This is the VLAN to which all source ports must be assigned.
- ◆ The VLAN specified by this command must be an existing VLAN configured with the **vlan** command.
- ◆ MVR source ports can be configured as members of the MVR VLAN using the **switchport allowed vlan** command and **switchport native vlan** command, but MVR receiver ports should not be statically configured as members of this VLAN.

## Example

The following example sets the MVR VLAN to VLAN 2:

```
Console(config)#mvr  
Console(config)#mvr domain 1 vlan 2  
Console(config)#
```



**mvr immediate-leave** This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

### Syntax

**mvr [domain *domain-id*] immediate-leave [by-host-ip]**

**no mvr [domain *domain-id*] immediate-leave**

*domain-id* - An independent multicast domain. (Range: 1-5)

**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

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- ◆ 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 (the same as it would without this option having been used). Instead of immediately deleting that group, it will look up the record, and only delete the group if there are no other subscribers for it on the member port. Only when all hosts on that port leave the group will the member port be deleted.
- ◆ Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- ◆ Immediate leave does not apply to multicast groups which have been statically assigned to a port with the **mvr vlan group** command.

### Example

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 immediate-leave
Console(config-if)#
```

**mvr type** This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

### Syntax

**[no] mvr [domain *domain-id*] type {receiver | source}**

*domain-id* - An independent multicast domain. (Range: 1-5)

**receiver** - Configures the interface as a subscriber port that can receive multicast data.

**source** - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

### Default Setting

The port type is not defined.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- ◆ Receiver ports can belong to different VLANs, but should not normally be configured as a member of the MVR VLAN. IGMP snooping can also be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see the [switchport mode](#) command).
- ◆ One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR protocol or which have been assigned through the [mvr vlan group](#) command.
- ◆ Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the [mvr vlan group](#) command.

### Example

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
```

```
Console(config-if)#mvr domain 1 type receiver  
Console(config-if)#
```

**mvr vlan group** This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

### Syntax

**[no] mvr [domain *domain-id*] vlan *vlan-id* group *ip-address***

*domain-id* - An independent multicast domain. (Range: 1-5)

*vlan-id* - Receiver VLAN to which the specified multicast traffic is flooded.  
(Range: 1-4094)

**group** - Defines a multicast service sent to the selected port.

*ip-address* - Statically configures an interface to receive multicast traffic from the IPv4 address specified for an MVR multicast group.  
(Range: 224.0.1.0 - 239.255.255.255)

### Default Setting

No receiver port is a member of any configured multicast group.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Multicast groups can be statically assigned to a receiver port using this command.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the **mvr vlan group** command.
- ◆ The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

### Example

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7  
Console(config-if)#mvr domain 1 type receiver  
Console(config-if)#mvr domain 1 vlan 3 group 225.0.0.5  
Console(config-if)#
```

**clear mvr groups dynamic** This command clears multicast group information dynamically learned through MVR.

#### Syntax

**clear mvr groups dynamic**

#### Command Mode

Privileged Exec

#### Command Usage

This command only clears entries learned through MVR. Statically configured multicast addresses are not cleared.

#### Example

```
Console#clear mvr groups r&d
Console#
```

**clear mvr statistics** This command clears MVR statistics.

#### Syntax

**clear mvr statistics** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

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

#### Command Mode

Privileged Exec

#### Example

```
Console#clear mvr statistics
Console#
```

**show mvr** This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

### Syntax

**show mvr** [**domain** *domain-id*]

*domain-id* - An independent multicast domain. (Range: 1-5)

### Default Setting

Displays configuration settings for all MVR domains.

### Command Mode

Privileged Exec

### Example

The following shows the MVR settings:

```

Console#show mvr
MVR 802.1p Forwarding Priority : Disabled
MVR Proxy Switching           : Enabled
MVR Robustness Value          : 1
MVR Proxy Query Interval      : 125(sec.)
MVR Source Port Mode          : Always Forward

MVR Domain                    : 1
MVR Config Status             : Enabled
MVR Running Status            : Active
MVR Multicast VLAN            : 1
MVR Current Learned Groups    : 10
MVR Upstream Source IP        : 192.168.0.3
:
```

**Table 131: show mvr - display description**

Field	Description
MVR 802.1p Forwarding Priority	Priority assigned to multicast traffic forwarded into the MVR VLAN
MVR Proxy Switching	Shows if MVR proxy switching is enabled
MVR Robustness Value	Shows the number of reports or query messages sent when proxy switching is enabled
MVR Proxy Query Interval	Shows the interval at which the receiver port sends out general queries
MVR Source Port Mode	Shows if the switch forwards all multicast streams, or only those which the source port has dynamically joined
MVR Domain	An independent multicast domain.
MVR Config Status	Shows if MVR is globally enabled on the switch.
MVR Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.)

Table 131: show mvr - display description (Continued)

Field	Description
MVR Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
MVR Current Learned Groups	The current number of MVR group addresses
MVR Upstream Source IP	The source IP address assigned to all upstream control packets.

**show mvr associated-profile** This command shows the profiles bound the specified domain.

#### Syntax

**show mvr [domain *domain-id*] associated-profile**

*domain-id* - An independent multicast domain. (Range: 1-5)

#### Default Setting

Displays profiles bound to all MVR domains.

#### Command Mode

Privileged Exec

#### Example

The following displays the profiles bound to domain 1:

```
Console#show mvr domain 1 associated-profile
Domain ID : 1
MVR Profile Name      Start IP Addr.  End IP Addr.
-----
rd                    228.1.23.1     228.1.23.10
testing              228.2.23.1     228.2.23.10
Console#
```

**show mvr interface** This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

#### Syntax

**show mvr [domain *domain-id*] interface**

*domain-id* - An independent multicast domain. (Range: 1-5)

#### Default Setting

Displays configuration settings for all attached interfaces.

#### Command Mode

Privileged Exec

### Example

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

```

Console#show mvr domain 1 interface
MVR Domain : 1
Flag: H - Immediate Leave By Host IP
Port      Type      Status              Immediate      Static Group Address
-----
Eth 1/ 1 Source  Active/Forwarding
Eth 1/ 2 Receiver Inactive/Discarding Disabled        234.5.6.8 (VLAN2)
Eth 1/ 3 Source  Inactive/Discarding
Eth 1/ 1 Receiver Active/Forwarding  Disabled        225.0.0.1 (VLAN1)
                                                225.0.0.9 (VLAN3)

Eth 1/ 4 Receiver Active/Discarding  Disabled
Console#

```

**Table 132: show mvr interface - display description**

Field	Description
MVR Domain	An independent multicast domain.
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is "ACTIVE" if MVR is globally enabled on the switch. MVR status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface. Also shows if MVR traffic is being forwarded or discarded.
Immediate	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR group assigned to an interface, and the receiver VLAN.

**show mvr members** This command shows information about the current number of entries in the forwarding database, detailed information about a specific multicast address, the IP address of the hosts subscribing to all active multicast groups, or the multicast groups associated with each port.

### Syntax

```

show mvr [domain domain-id] members [ip-address |
host-ip-address [interface] | igmp | sort-by-port [interface | unknown |
user]]]

```

*domain-id* - An independent multicast domain. (Range: 1-5)

*ip-address* - IPv4 address for an MVR multicast group.  
(Range: 224.0.1.0 - 239.255.255.255)

**members** - The multicast groups assigned to the MVR VLAN.

**host-ip-address** - The subscriber IP addresses.

**igmp** - Entry created by IGMP protocol.

**sort-by-port** - The multicast groups associated with an interface.  
*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

**unknown** - Entry created by receiving a multicast stream.

**user** - Snooping entry learned from user's configuration settings.

### Default Setting

Displays configuration settings for all domains and all forwarding entries.

### Command Mode

Privileged Exec

### Example

The following shows information about the number of multicast forwarding entries currently active in domain 1:

```
Console#show mvr domain 1 members
MVR Domain : 1
MVR Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts joined to group on this port).
      P - Port counts (number of ports joined to group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address   VLAN Port           Up time           Expire Count
-----
234.5.6.7       1                   00:00:09:17      2 (P)
                  1 Eth 1/ 1(S)
                  2 Eth 1/ 2(R)

Console#
```

The following example shows detailed information about a specific multicast address:

```
Console#show mvr domain 1 members 234.5.6.7
MVR Domain : 1
MVR Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts joined to group on this port).
      P - Port counts (number of ports joined to group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).
```



```

Group Address   VLAN Port           Up time           Expire Count
-----
234.5.6.7      1                   1 Eth 1/ 1(S)    2(P)
                2 Eth 1/ 2(R)

```

Console#

**Table 133: show mvr members - display description**

Field	Description
Group Address	Multicast group address.
VLAN	VLAN to which this address is forwarded.
Port	Port to which this address is forwarded.
Uptime	Time that this multicast group has been known.
Expire	The time until this entry expires.
Count	The number of times this address has been learned by IGMP snooping.

**show mvr profile** This command shows all configured MVR profiles.

### Command Mode

Privileged Exec

### Example

The following shows all configured MVR profiles:

```

Console#show mvr profile
MVR Profile Name   Start IP Addr.   End IP Addr.
-----
rd                 228.1.23.1      228.1.23.10
testing            228.2.23.1      228.2.23.10
Console#

```

**show mvr statistics** This command shows MVR protocol-related statistics for the specified interface.

### Syntax

```
show mvr [domain domain-id] statistics
  {input [interface interface] | output [interface interface] |
  query | summary interface [interface]}
```

*domain-id* - An independent multicast domain. (Range: 1-5)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

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

**query** - Displays MVR query-related statistics.

**summary** - Displays summary of MVR statistics.

### Default Setting

Displays statistics for all domains.

### Command Mode

Privileged Exec

### Example

The following shows MVR protocol-related statistics received:

```
Console#show mvr domain 1 statistics input
MVR Domain : 1 , MVR VLAN: 2
Input Statistics:
Interface Report   Leave    G Query  G(-S)-S Query Drop      Join Succ Group
-----
Eth 1/ 1          23       11       4         10       5        20    9
Eth 1/ 2          12       15       8         3        5        19    4
DVLAN  1           2         0         0         2        2        20    9
MVLAN  1           2         0         0         2        2        20    9
Console#
```

**Table 134: show mvr statistics input - display description**

Field	Description
Interface	Shows interfaces attached to the MVR.
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.

**Table 134: show mvr statistics input - display description** (Continued)

Field	Description
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 MVR group report received
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MVR groups active on this interface.

The following shows MVR protocol-related statistics sent:

```

Console#show mvr domain 1 statistics output
MVR Domain : 1 , MVR VLAN: 2
Output Statistics:
Interface  Report  Leave   G Query  G(-S)-S Query  Drop    Group
-----
Eth 1/ 1   12      0       1        0             0       0
Eth 1/ 1   12      0       1        0             0       0
Eth 1/ 2    5       1       4        1             0       0
DVLAN  1    7       2       3        0             0       0
MVLAN  1    7       2       3        0             0       0
Console#

```

**Table 135: show mvr statistics output - display description**

Field	Description
Interface	Shows interfaces attached to the MVR.
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 MVR query-related statistics:

```

Console#show mvr domain 1 statistics query
Domain 1:
  Other Querier           : None
  Other Querier Expire    : 0(m):0(s)
  Other Querier Uptime    : 0(h):0(m):0(s)
  Self Querier            : 192.168.2.4
  Self Querier Expire     : 0(m):30(s)
  Self Querier Uptime     : 0(h):9(m):55(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 136: show mvr statistics query - display description**

Field	Description
Other Querier	The IP address of the querier on this interface.
Other Querier Expire	The time after which this querier is assumed to have expired.
Other Querier Uptime	Other querier's time up.
Self Querier	This querier's IP address.
Self Querier Expire	This querier's expire time.
Self Querier Uptime	This querier's time 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.
Warn Rate Limit	Count down from 15 seconds after receiving a Query different from the configured version.
V# Warning Count	Number of queries received on MVR that were configured for IGMP version 1, 2 or 3.

The following shows MVR summary statistics for an interface:

```

Console#show mvr domain 1 statistics summary interface ethernet 1/1
Domain 1:
Number of Groups: 0
Querier:          :                               Report & Leave:  :
  Transmit        :                               Transmit        :
    General        : 0                             Report          : 7
    Group Specific : 0                             Leave           : 4
Received         :                               Received        :
  General          : 0                             Report          : 0
  Group Specific   : 0                             Leave           : 0
  V1 Warning Count: 0                             Join Success    : 0
  V2 Warning Count: 0                             Filter Drop     : 0
  V3 Warning Count: 0
                                           Source Port Drop: 0
                                           Others Drop      : 0

Console#

```

**Table 137: show mvr statistics summary interface - display description**

Field	Description
Domain	An independent multicast domain.
Number of Groups	Number of groups learned on this port.
Querier	
Transmit	
General	Number of general queries transmitted.
Group Specific	Number of group specific queries transmitted.
Received	
General	Number of general queries received.
Group Specific	Number of group specific queries received.
V# Warning Count	Number of queries received on MVR that were configured for IGMP version 1, 2 or 3.
Report & Leave	
Transmit	
Report	Number of transmitted reports.
Leave	Number of transmitted leaves.
Received	
Report	Number of reports received.
Leave	Number of leaves received.
Join Success	Number of join reports processed successfully.
Filter Drop	Number of report/leave messages dropped by IGMP filter.
Source Port Drop	Number of report/leave messages dropped by MVR source port.
Others Drop	Number of report/leave messages dropped for other reasons.

## MVR for IPv6

This section describes commands used to configure Multicast VLAN Registration for IPv6 (MVR6). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR6 VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR6 maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

**Table 138: Multicast VLAN Registration for IPv6 Commands**

Command	Function	Mode
<code>mvr6 associated-profile</code>	Binds the MVR6 group addresses specified in a profile to an MVR6 domain	GC
<code>mvr6 domain</code>	Enables MVR6 for a specific domain	GC
<code>mvr6 priority</code>	Assigns a priority to all multicast traffic in the MVR6 VLAN	GC
<code>mvr6 profile</code>	Maps a range of MVR6 group addresses to a profile	GC
<code>mvr6 proxy-query-interval</code>	Configures the interval at which the receiver port sends out general queries.	GC
<code>mvr6 proxy-switching</code>	Enables MVR6 proxy switching, where the source port acts as a host, and the receiver port acts as an MVR6 router with querier service enabled	GC
<code>mvr6 robustness-value</code>	Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries	GC
<code>mvr6 source-port-mode dynamic</code>	Configures the switch to only forward multicast streams which the source port has dynamically joined	GC
<code>mvr6 upstream-source-ip</code>	Configures the source IP address assigned to all control packets sent upstream	GC
<code>mvr6 vlan</code>	Specifies the VLAN through which MVR6 multicast data is received	GC
<code>mvr6 immediate-leave</code>	Enables immediate leave capability	IC
<code>mvr6 type</code>	Configures an interface as an MVR6 receiver or source port	IC
<code>mvr6 vlan group</code>	Statically binds a multicast group to a port	IC
<code>clear mvr6 groups dynamic</code>	Clears multicast group information dynamically learned through MVR6	PE
<code>clear mvr6 statistics</code>	Clears the MVR6 statistics globally or on a per-interface basis	PE
<code>show mvr6</code>	Shows information about MVR6 domain settings, including MVR6 operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address	PE
<code>show mvr6 associated-profile</code>	Shows the profiles bound the specified domain	PE
<code>show mvr6 interface</code>	Shows MVR6 settings for interfaces attached to the MVR6 VLAN	PE

**Table 138: Multicast VLAN Registration for IPv6 Commands** (Continued)

Command	Function	Mode
<code>show mvr6 members</code>	Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address	PE
<code>show mvr6 profile</code>	Shows all configured MVR6 profiles	PE
<code>show mvr6 statistics</code>	Shows MVR6 protocol statistics for the specified interface	PE

**mvr6 associated-profile** This command binds the MVR6 group addresses specified in a profile to an MVR6 domain. Use the **no** form of this command to remove the binding.

### Syntax

**[no] mvr6 domain** *domain-id* **associated-profile** *profile-name*

*domain-id* - An independent multicast domain. (Range: 1-5)

*profile-name* - The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

### Example

The following an MVR6 group address profile to domain 1:

```
Console(config)#mvr6 domain 1 associated-profile rd
Console(config)#
```

**mvr6 domain** This command enables Multicast VLAN Registration for IPv6 (MVR6) for a specific domain. Use the **no** form of this command to disable MVR6 for a domain.

### Syntax

**[no] mvr6 domain** *domain-id*

*domain-id* - An independent multicast domain. (Range: 1-5)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

When MVR6 is enabled on a domain, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group.

### Example

The following example enables MVR6 for domain 1:

```
Console(config)#mvr6 domain 1
Console(config)#
```

**mvr6 priority** This command assigns a priority to all multicast traffic in the MVR6 VLAN. Use the **no** form of this command to restore the default setting.

### Syntax

**mvr6 priority** *priority*

**no mvr6 priority**

*priority* - The CoS priority assigned to all multicast traffic forwarded into the MVR6 VLAN. (Range: 0-7, where 7 is the highest priority)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

### Example

```
Console(config)#mvr6 priority 6
Console(config)#
```

### Related Commands

[show mvr6 \(674\)](#)



**mvr6 profile** This command maps a range of MVR6 group addresses to a profile. Use the **no** form of this command to remove the profile.

### Syntax

**mvr6 profile** *profile-name start-ip-address end-ip-address*

*profile-name* - The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)

*start-ip-address* - Starting IPv6 address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

*end-ip-address* - Ending IPv6 address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

### Default Setting

No profiles are defined

### Command Mode

Global Configuration

### Command Usage

- ◆ Use this command to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.
- ◆ IGMP snooping and MVR6 share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.
- ◆ 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. (Note that the IP address ff02::X is reserved.)
- ◆ The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

### Example

The following example maps a range of MVR6 group addresses to a profile:

```
Console(config)#mvr6 profile rd ff01:0:0:0:0:0:fe ff01:0:0:0:0:0:ff
Console(config)#
```

**mvr6 proxy-query-interval** This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

#### Syntax

**mvr6 proxy-query-interval** *interval*

**no mvr6 proxy-query-interval**

*interval* - The interval at which the receiver port sends out general queries.  
(Range: 2-31744 seconds)

#### Default Setting

125 seconds

#### Command Mode

Global Configuration

#### Command Usage

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the [mvr6 proxy-switching](#) command.

#### Example

This example sets the proxy query interval for MVR6.

```
Console(config)#mvr6 proxy-query-interval 1000
Console(config)#
```

**mvr6 proxy-switching** This command enables MVR6 proxy switching, where the source port acts as a host, and the receiver port acts as an MVR6 router with querier service enabled. Use the **no** form to disable this function.

#### Syntax

**[no] mvr6 proxy-switching**

#### Default Setting

Enabled

#### Command Mode

Global Configuration

#### Command Usage

- ◆ When MVR6 proxy-switching is enabled, an MVR6 source port serves as the upstream or host interface, and the MVR6 receiver port serves as the querier. The source port performs only the host portion of MVR6 by sending summarized membership reports, and automatically disables MVR6 router functions.

- ◆ Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR6 router functions by maintaining a database of all MVR6 subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR6 proxy service.
- ◆ When the source port receives report and leave messages, it only forwards them to other source ports.
- ◆ When receiver ports receive any query messages, they are dropped.
- ◆ When changes occurring in the downstream MVR6 groups are learned by the receiver ports through report and leave messages, an MVR6 state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- ◆ When MVR6 proxy switching is disabled:
  - Any membership reports received from receiver/source ports are forwarded to all source ports.
  - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
  - When a receiver port receives a query message, it will be dropped.

### Example

The following example enable MVR6 proxy switching.

```
Console(config)#mvr6 proxy-switching
Console(config)#
```

### Related Commands

[mvr6 robustness-value \(667\)](#)

**mvr6 robustness-value** This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the **no** form to restore the default setting.

### Syntax

**mvr6 robustness-value** *value*

**no mvr6 robustness-value**

*value* - The robustness used for all interfaces. (Range: 1-10)

### Default Setting

2

### Command Mode

Global Configuration

### Command Usage

- ◆ This command sets the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- ◆ This command only takes effect when MVR6 proxy switching is enabled.

### Example

```
Console(config)#mvr6 robustness-value 5  
Console(config)#
```

### Related Commands

[mvr6 proxy-switching \(666\)](#)

**mvr6 source-port-mode dynamic** This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

### Syntax

**[no] mvr6 source-port-mode dynamic**

### Default Setting

Forwards all multicast streams which have been specified in a profile and bound to a domain.

### Command Mode

Global Configuration

### Command Usage

- ◆ By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- ◆ When the **mvr6 source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

### Example

```
Console(config)#mvr6 source-port-mode dynamic
Console(config)#
```

**mvr6 upstream-source-ip** This command configures the source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. Use the **no** form to restore the default setting.

### Syntax

**mvr6 domain** *domain-id* **upstream-source-ip** *source-ip-address*

**no mvr6 domain** *domain-id* **upstream-source-ip**

*domain-id* - An independent multicast domain. (Range: 1-5)

*source-ip-address* – The source IPv6 address assigned to all MVR6 control packets sent upstream. This parameter must be a full IPv6 address including the network prefix and host address bits.

### Default Setting

All MVR6 reports sent upstream use a null source IP address

### 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. (Note that the IP address ff02::X is reserved.)

### Example

```
Console(config)#mvr6 domain 1 upstream-source-ip 2001:DB8:2222:7223::72
Console(config)#
```

**mvr6 vlan** This command specifies the VLAN through which MVR6 multicast data is received. Use the **no** form of this command to restore the default MVR6 VLAN.

### Syntax

**mvr6 domain** *domain-id* **vlan** *vlan-id*

**no mvr6 domain** *domain-id* **vlan**

*domain-id* - An independent multicast domain. (Range: 1-5)

*vlan-id* - Specifies the VLAN through which MVR6 multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

### Default Setting

VLAN 1

### Command Mode

Global Configuration

### Command Usage

MVR6 source ports can be configured as members of the MVR6 VLAN using the `switchport allowed vlan` command and `switchport native vlan` command, but MVR6 receiver ports should not be statically configured as members of this VLAN.

### Example

The following example sets the MVR6 VLAN to VLAN 1:

```
Console(config)#mvr6 domain 1 vlan 1
Console(config)#
```

**mvr6 immediate-leave** This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

### Syntax

**[no] mvr6 domain *domain-id* immediate-leave [by-host-ip]**

*domain-id* - An independent multicast domain. (Range: 1-5)

**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

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

- ◆ If the “by-host-ip” option is enabled, the switch will not send out a group-specific query to the receiver port. But it 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.
- ◆ Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- ◆ Immediate leave does not apply to multicast groups which have been statically assigned to a port with the `mvr6 vlan group` command.

### Example

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 immediate-leave
Console(config-if)#
```

**mvr6 type** This command configures an interface as an MVR6 receiver or source port. Use the **no** form to restore the default settings.

### Syntax

**[no] mvr6 domain** *domain-id* **type** {**receiver** | **source**}

*domain-id* - An independent multicast domain. (Range: 1-5)

**receiver** - Configures the interface as a subscriber port that can receive multicast data.

**source** - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups. Note that the source port must be manually configured as a member of the MVR6 VLAN using the `switchport allowed vlan` command.

### Default Setting

The port type is not defined.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6. A port which is not configured as an MVR6 receiver or source port can use MLD snooping to join or leave multicast groups using the standard rules for multicast filtering (see “[MLD Snooping](#)” on [page 614](#)).

- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR6 VLAN. MLD snooping can be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR6 VLAN. Also, note that VLAN membership for MVR6 receiver ports cannot be set to access mode (see the `switchport mode` command).
- ◆ One or more interfaces may be configured as MVR6 source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR6 protocol or which have been assigned through the `mvr6 vlan group` command.  
All source ports must belong to the MVR6 VLAN.  
Subscribers should not be directly connected to source ports.
- ◆ The same port cannot be configured as a source port in one MVR6 domain and as a receiver port in another domain.

### Example

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#
```

**mvr6 vlan group** This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

### Syntax

**[no] mvr6 domain** *domain-id* **vlan** *vlan-id* **group** *ip-address*

*domain-id* - An independent multicast domain. (Range: 1-5)

*vlan-id* - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

**group** - Defines a multicast service sent to the selected port.

*ip-address* - Statically configures an interface to receive multicast traffic from the IPv6 address specified for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

### Default Setting

No receiver port is a member of any configured multicast group.



### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Multicast groups can be statically assigned to a receiver port using this command. The assigned address must fall within the range set by the `mvr6 associated-profile` command.
- ◆ 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. (Note that the IP address `ff02::X` is reserved.)
- ◆ The MVR6 VLAN cannot be specified as the receiver VLAN for static bindings.

### Example

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/2
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1
Console(config-if)#
```

**clear mvr6 groups dynamic** This command clears multicast group information dynamically learned through MVR6.

### Syntax

**clear mvr6 groups dynamic** *domain-id*

*domain-id* - An independent multicast domain. (Range: 1-5)

### Command Mode

Privileged Exec

### Command Usage

This command only clears entries learned through MVR6. Statically configured multicast addresses are not cleared.

### Example

```
Console#clear mvr6 groups r&d
Console#
```

**clear mvr6 statistics** This command clears MVR6 statistics.

### Syntax

**clear mvr statistics** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

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

### Command Mode

Privileged Exec

### Command Usage

If the interface option is not used then all MVR6 statistics are cleared. Otherwise using the interface option will only clear MVR6 statistics for the specified interface.

### Example

```
Console#clear mvr6 statistics
Console#
```

**show mvr6** This command shows information about MVR6 domain settings, including MVR6 operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

### Syntax

**show mvr6** [**domain** *domain-id*]

*domain-id* - An independent multicast domain. (Range: 1-5)

### Default Setting

Displays configuration settings for all MVR6 domains.

### Command Mode

Privileged Exec

### Example

The following shows the MVR6 settings:

```
Console#show mvr6
MVR6 802.1p Forwarding Priority: Disabled
MVR6 Proxy Switching          : Enabled
MVR6 Robustness Value         : 1
```

```

MVR6 Proxy Query Interval      : 125(sec.)
MVR6 Source Port Mode          : Always Forward

Domain                          : 1
MVR6 Config Status             : Enabled
MVR6 Running Status            : Active
MVR6 Multicast VLAN            : 1
MVR6 Current Learned Groups    : 0
MVR6 Upstream Source IP        : FF05::25
Console#

```

**Table 139: show mvr6 - display description**

Field	Description
MVR6 802.1p Forwarding Priority	Priority assigned to multicast traffic forwarded into the MVR6 VLAN
MVR Proxy Switching	Shows if MVR proxy switching is enabled
MVR6 Robustness Value	Shows the number of reports or query messages sent when proxy switching is enabled
MVR6 Proxy Query Interval	The interval at which the receiver port sends out general queries
MVR6 Source Port Mode	Shows if the switch only forwards multicast streams which the source port has dynamically joined or always forwards multicast streams
MVR6 Domain	An independent multicast domain.
MVR6 Config Status	Shows if MVR is globally enabled on the switch.
MVR6 Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists, and a source port with a valid link has been configured (using the <a href="#">mvr6 type</a> command.)
MVR6 Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
MVR Current Learned Groups	The current number of MVR group addresses
MVR6 Upstream Source IP	The source IP address assigned to all upstream control packets.

**show mvr6 associated-profile** This command shows the profiles bound the specified domain.

**Syntax**

**show mvr6 [domain *domain-id*] associated-profile**

*domain-id* - An independent multicast domain. (Range: 1-5)

**Default Setting**

Displays profiles bound to all MVR6 domains.

**Command Mode**

Privileged Exec

### Example

The following displays the profiles bound to domain 1:

```
Console#show mvr6 domain 1 associated-profile
Domain ID : 1
MVR6 Profile Name      Start IPv6 Addr.      End IPv6 Addr.
-----
rd                      ff01::fe              ff01::ff
Console#
```

**show mvr6 interface** This command shows MVR6 configuration settings for interfaces attached to the MVR6 VLAN.

### Syntax

**show mvr6 [domain *domain-id*] interface**

*domain-id* - An independent multicast domain. (Range: 1-5)

### Default Setting

Displays configuration settings for all attached interfaces.

### Command Mode

Privileged Exec

### Example

The following displays information about the interfaces attached to the MVR6 VLAN in domain 1:

```
Console#show mvr6 domain 1 interface
MVR6 Domain : 1
Port      Type      Status              Immediate Leave  Static Group Address
-----
Eth1/ 1   Source   Active/Forwarding
Eth1/ 2   Receiver Active/Forwarding  Disabled         ff00::1 (VLAN1)
Console#
```

**Table 140: show mvr6 interface - display description**

Field	Description
Port	Shows interfaces attached to the MVR6.
Type	Shows the MVR6 port type.
Status	Shows the MVR6 status and interface status. MVR6 status for source ports is "ACTIVE" if MVR6 is globally enabled on the switch. MVR6 status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR6 groups, or a multicast group has been statically assigned to an interface.

**Table 140: show mvr6 interface - display description** (Continued)

Field	Description
Immediate Leave	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR6 group assigned to an interface, and the receiver VLAN.

**show mvr6 members** This command shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address.

### Syntax

**show mvr6** [**domain** *domain-id*] **members** [*ip-address*]

*domain-id* - An independent multicast domain. (Range: 1-5)

*ip-address* - IPv6 address for an MVR6 multicast group.

### Default Setting

Displays configuration settings for all domains and all forwarding entries.

### Command Mode

Privileged Exec

### Example

The following shows information about the number of multicast forwarding entries currently active in domain 1:

```

Console#show mvr6 domain 1 members
MVR6 Domain : 1
MVR6 Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of forwarding ports).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address          VLAN Port          Up time          Expire Count
-----
ff05::101              2                  00:00:00:19     2(P)
                       2 Eth1/ 1(S)
                       1 Eth1/ 2(R)
                       1                  0(H)

Console#

```

The following example shows detailed information about a specific multicast address:

```

Console#show mvr6 domain 1 members ff00::1
MVR6 Domain : 1
MVR6 Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts join the group on this port).

```

```

P - Port counts (number of forwarding ports).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address          VLAN Port          Up time          Expire Count
-----
ff05::101              2                  00:00:03:18     2 (P)
                       2 Eth1/ 2 (S)
                       1 Eth1/ 4 (R)
Console#

```

**Table 141: show mvr6 members - display description**

Field	Description
Group Address	Multicast group address.
VLAN	VLAN to which this address is forwarded.
Port	Port to which this address is forwarded.
Up time	Time that this multicast group has been known.
Expire	The time until this entry expires.
Count	The number of times this address has been learned by MVR (MLD snooping).

**show mvr6 profile** This command shows all configured MVR6 profiles.

**Command Mode**  
Privileged Exec

**Example**  
The following shows all configured MVR6 profiles:

```

Console#show mvr6 profile
MVR6 Profile Name      Start IPv6 Addr.      End IPv6 Addr.
-----
rd                      ff01::fe              ff01::ff
Console#

```

**show mvr6 statistics** This command shows MVR protocol-related statistics for the specified interface.

### Syntax

**show mvr6 statistics** {input | output} [interface *interface*]

**show mvr6 domain** *domain-id* **statistics**  
{input [interface *interface*] | output [interface *interface*] |  
**query**}

*domain-id* - An independent multicast domain. (Range: 1-5)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

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

**query** - Displays MVR query-related statistics.

### Default Setting

Displays statistics for all domains.

### Command Mode

Privileged Exec

### Example

The following shows MVR6 protocol-related statistics received:

```

Console#show mvr6 domain 1 statistics input
MVR Domain : 1
Input Statistics:
Interface Report    Leave    G Query    G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23       11         4           10       5         20       9
Eth 1/ 2           12       15         8           3         5         19       4
MVLAN 2            2         0          0           2         2         20       9
Console#

```

**Table 142: show mvr6 statistics input - display description**

Field	Description
Interface	Shows interfaces attached to the MVR.
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.

**Table 142: show mvr6 statistics input - display description** (Continued)

Field	Description
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 MVR group report received
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MVR groups active on this interface.

The following shows MVR6 protocol-related statistics sent:

```

Console#show mvr6 domain 1 statistics output
MVR Domain : 1
Output Statistics:
Interface Report      Leave      G Query    G(-S)-S Query
-----
Eth 1/ 1              12         0          1           0
Eth 1/ 2               5         1          4           1
MVLAN 1               7         2          3           0
Console#

```

**Table 143: show mvr6 statistics output - display description**

Field	Description
Interface	Shows interfaces attached to the MVR.
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.
Group	The number of MVR groups active on this interface.

The following shows MVR6 query-related statistics:

```

Console#show mvr6 domain 1 statistics query
Other Querier Address      : None
Other Querier Uptime       : 0(h):0(m):0(s)
Other Querier Expire Time  : 0(m):0(s)
Self Querier Address       : 2001:db8:2222:7272::
Self Querier Uptime        : 0(h):0(m):0(s)
Self Querier Expire Time   : 0(m):0(s)
General Query Received     : 0
General Query Sent         : 0
Specific Query Received    : 0
Specific Query Sent        : 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 144: 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 144: 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 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 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\*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** *packets*

**no lldp med-fast-start-count**

*seconds* - 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)#
```

**lldp refresh-interval** This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

### Syntax

**lldp refresh-interval** *seconds*

**no lldp 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)#
```

**lldp 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

**lldp reinit-delay** *seconds*

**no lldp 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 504](#)).

**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 483 and “[protocol-vlan protocol-group \(Configuring Interfaces\)](#)” on page 506.

**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, Port Channel)

**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, Port Channel)

### 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, Port Channel)

### Command Usage

Refer to [“Frame Size” on page 102](#) 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 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 145: 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

Table 145: LLDP MED Location CA Types (Continued)

CA Type	Description	CA Value Example
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 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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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
                             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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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 : ECS4100-26TX
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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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
Local Port 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   : ECS2100-28PP
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: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### 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#
```

---



## CFM Commands

Connectivity Fault Management (CFM) is an OAM protocol that includes proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between provider edge devices or between customer edge devices.

CFM is implemented as a service level protocol based on service instances which encompass only that portion of the metropolitan area network supporting a specific customer. CFM can also provide controlled management access to a hierarchy of maintenance domains (such as the customer, service provider, and equipment operator).

The following list of commands support functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also provides commands for fault detection through continuity check messages for all known maintenance points, and cross-check messages for statically configured maintenance points located on other devices. Fault verification is supported through loop back messages, and fault isolation through link trace messages. Fault notification is also provided by SNMP alarms which are automatically generated by maintenance points when connectivity faults or configuration errors are detected in the local maintenance domain.

**Table 146: CFM Commands**

Command	Function	Mode
<i>Defining CFM Structures</i>		
<code>ethernet cfm ais level</code>	Configures the maintenance level at which Alarm Indication Signal information will be sent	GC
<code>ethernet cfm ais ma</code>	Enables the MEPs within the specified MA to send frames with AIS information	GC
<code>ethernet cfm ais period</code>	Configures the interval at which AIS information is sent	GC
<code>ethernet cfm ais suppress alarm</code>	Suppresses AIS messages following the detection of defect conditions	GC
<code>ethernet cfm domain</code>	Defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode; also specifies the MIP creation method for MAs within this domain	GC
<code>ethernet cfm enable</code>	Enables CFM processing globally on the switch	GC
<code>ma index name</code>	Creates a maintenance association within the current maintenance domain, maps it to a customer service instance, and sets the manner in which MIPs are created for this service instance	CFM

Table 146: CFM Commands (Continued)

Command	Function	Mode
<code>ma index name-format</code>	Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format	CFM
<code>ethernet cfm mep</code>	Sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages	IC
<code>ethernet cfm port-enable</code>	Enables CFM processing on an interface	IC
<code>clear ethernet cfm ais mpid</code>	Clears AIS defect information for the specified MEP	PE
<code>show ethernet cfm configuration</code>	Displays CFM configuration settings, including global settings, SNMP traps, and interface settings	PE
<code>show ethernet cfm md</code>	Displays configured maintenance domains	PE
<code>show ethernet cfm ma</code>	Displays configured maintenance associations	PE
<code>show ethernet cfm maintenance-points local</code>	Displays maintenance points configured on this device	PE
<code>show ethernet cfm maintenance-points local detail mep</code>	Displays detailed CFM information about a specified local MEP in the continuity check database	PE
<code>show ethernet cfm maintenance-points remote detail</code>	Displays detailed CFM information about a specified remote MEP in the continuity check database	PE
<i>Continuity Check Operations</i>		
<code>ethernet cfm cc ma interval</code>	Sets the transmission delay between continuity check messages	GC
<code>ethernet cfm cc enable</code>	Enables transmission of continuity check messages within a specified maintenance association	GC
<code>snmp-server enable traps ethernet cfm cc</code>	Enables SNMP traps for CFM continuity check events	GC
<code>mep archive-hold-time</code>	Sets the time that data from a missing MEP is kept in the continuity check database before being purged	CFM
<code>clear ethernet cfm maintenance-points remote</code>	Clears the contents of the continuity check database	PE
<code>clear ethernet cfm errors</code>	Clears continuity check errors logged for the specified maintenance domain and maintenance level	PE
<code>show ethernet cfm errors</code>	Displays CFM continuity check errors logged on this device	PE
<i>Cross Check Operations</i>		
<code>ethernet cfm mep crosscheck start-delay</code>	Sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation	GC
<code>snmp-server enable traps ethernet cfm crosscheck</code>	Enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages	GC
<code>mep crosscheck mpid</code>	Statically defines a remote MEP in a maintenance association	CFM

Table 146: CFM Commands (Continued)

Command	Function	Mode
<code>ethernet cfm mep crosscheck</code>	Enables cross-checking between the list of configured remote MEPs within a maintenance association and MEPs learned through continuity check messages	PE
<code>show ethernet cfm maintenance-points remote crosscheck</code>	Displays information about remote maintenance points configured statically in a cross-check list	PE
<i>Link Trace Operations</i>		
<code>ethernet cfm linktrace cache</code>	Enables caching of CFM data learned through link trace messages	GC
<code>ethernet cfm linktrace cache hold-time</code>	Sets the hold time for CFM link trace cache entries	GC
<code>ethernet cfm linktrace cache size</code>	Sets the maximum size for the link trace cache	GC
<code>ethernet cfm linktrace</code>	Sends CFM link trace messages to the MAC address for a MEP	PE
<code>clear ethernet cfm linktrace-cache</code>	Clears link trace messages logged on this device	PE
<code>show ethernet cfm linktrace-cache</code>	Displays the contents of the link trace cache	PE
<i>Loopback Operations</i>		
<code>ethernet cfm loopback</code>	Sends CFM loopback messages to a MAC address for a MEP or MIP	PE
<i>Fault Generator Operations</i>		
<code>mep fault-notify alarm-time</code>	Sets the time a defect must exist before a fault alarm is issued	CFM
<code>mep fault-notify lowest-priority</code>	Sets the lowest priority defect that is allowed to generate a fault alarm	CFM
<code>mep fault-notify reset-time</code>	Configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued	CFM
<code>show ethernet cfm fault-notify-generator</code>	Displays configuration settings for the fault notification generator	PE
<i>Delay Measure Operations</i>		
<code>ethernet cfm delay-measure two-way</code>	Sends periodic delay-measure requests to a specified MEP within a maintenance association	PE

*Basic Configuration Steps for CFM*

1. Configure the maintenance domains with the `ethernet cfm domain` command.
2. Configure the maintenance associations with the `ma index name` command.
3. Configure the local maintenance end points (MEPs) which will serve as the domain service access points for the specified maintenance association using the `ethernet cfm mep` command.

4. Enter a static list of MEPs assigned to other devices within the same maintenance association using the `mep crosscheck mpid` command. This allows CFM to automatically verify the functionality of these remote end points by cross-checking the static list configured on this device against information learned through continuity check messages.
5. Enable CFM globally on the switch with the `ethernet cfm enable` command.
6. Enable CFM on the local MEPs with the `ethernet cfm port-enable` command.
7. Enable continuity check operations with the `ethernet cfm cc enable` command.
8. Enable cross-check operations with the `ethernet cfm mep crosscheck` command.

Other configuration changes may be required for your particular environment, such as adjusting the interval at which continuity check messages are sent (page 725), or setting the start-up delay for the cross-check operation (page 731). You can also enable SNMP traps for events discovered by continuity check messages (page 727) or cross-check messages (page 731).

## Defining CFM Structures

**ethernet cfm ais level** This command configures the maintenance level at which Alarm Indication Signal (AIS) information will be sent within the specified MA. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm ais level** *level-id* **md** *domain-name* **ma** *ma-name*

**no ethernet cfm ais level md** *domain-name* **ma** *ma-name*

*level-id* – Maintenance level at which AIS information will be sent.  
(Range: 0-7)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

Level 0

### Command Mode

Global Configuration

### Command Usage

The configured AIS level must be higher than the maintenance level of the domain containing the specified MA.

### Example

This example sets the maintenance level for sending AIS messages within the specified MA.

```
Console(config)#ethernet cfm ais level 4 md voip ma rd
Console(config)#
```

**ethernet cfm ais ma** This command enables the MEPs within the specified MA to send frames with AIS information following detection of defect conditions. Use the **no** form to disable this feature.

### Syntax

**[no] ethernet cfm ais md** *domain-name* **ma** *ma-name*

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name<sup>13</sup>. (Range: 1-43 alphanumeric characters)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ Each MA name must be unique within the CFM domain.
- ◆ Frames with AIS information can be issued at the client's maintenance level by a MEP upon detecting defect conditions. For example, defect conditions may include:
  - Signal failure conditions if continuity checks are enabled.
  - AIS condition or LCK condition if continuity checks are disabled.
- ◆ A MEP continues to transmit periodic frames with AIS information until the defect condition is removed.

### Example

This example enables the MEPs within the specified MA to send frames with AIS information.

```
Console(config)#ethernet cfm ais md voip ma rd
Console(config)#
```

13. The total length of the MD name and MA name cannot exceed 44 characters.

**ethernet cfm ais period** This command configures the interval at which AIS information is sent. Use the **no** form to restore the default setting.

#### Syntax

**ethernet cfm ais period** *period* **md** *domain-name* **ma** *ma-name*

**no ethernet cfm ais period md** *domain-name* **ma** *ma-name*

*period* – The interval at which AIS information is sent.  
(Options: 1 second, 60 seconds)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

#### Default Setting

1 second

#### Command Mode

Global Configuration

#### Example

This example sets the interval for sending frames with AIS information at 60 seconds.

```
Console(config)#ethernet cfm ais period 60 md voip ma rd
Console(config)#
```

**ethernet cfm ais suppress alarm** This command suppresses sending frames containing AIS information following the detection of defect conditions. Use the **no** form to restore the default setting.

#### Syntax

**[no] ethernet cfm ais suppress alarm md** *domain-name* **ma** *ma-name*

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

#### Default Setting

Suppression is disabled

#### Command Mode

Global Configuration

#### Command Usage

- ◆ For multipoint connectivity, a MEP cannot determine the specific maintenance level entity that has encountered defect conditions upon receiving a frame

with AIS information. More importantly, it cannot determine the associated subset of its peer MEPs for which it should suppress alarms since the received AIS information does not contain that information. Therefore, upon reception of a frame with AIS information, the MEP will suppress alarms for all peer MEPs whether there is still connectivity or not.

- ◆ However, for a point-to-point connection, a MEP has only a single peer MEP for which to suppress alarms when it receives frames with AIS information.
- ◆ If suppression is enabled by this command, upon receiving a frame with AIS information, a MEP detects an AIS condition and suppresses loss of continuity alarms associated with all its peer MEPs. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of AIS messages.

### Example

This example suppresses sending frames with AIS information.

```
Console(config)#ethernet cfm ais suppress alarm md voip ma rd
Console(config)#
```

**ethernet cfm domain** This command defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode. Use the **no** form to delete a CFM maintenance domain.

### Syntax

**ethernet cfm domain index** *index* **name** *domain-name* **level** *level-id*  
[**mip-creation** *type*]

**no ethernet cfm domain index** *index*

*index* – Domain index. (Range: 1-65535)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Authorized maintenance level for this domain. (Range: 0-7)

*type* – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:

**default** – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.

**explicit** – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

**none** – No MIP can be created for any MA configured in this domain.

### Default Setting

No maintenance domains are configured.  
No MIPs are created for any MA in the specified domain.

### Command Mode

Global Configuration

### Command Usage

- ◆ A domain can only be configured with one name.
- ◆ Where domains are nested, an upper-level hierarchical domain must have a higher maintenance level than the ones it encompasses. The higher to lower level domain types commonly include entities such as customer, service provider, and operator.
- ◆ More than one domain can be configured at the same maintenance level, but a single domain can only be configured with one maintenance level.
- ◆ If MEPs or MAs are configured for a domain using the `ethernet cfm mep` command or `ma index name` command, they must first be removed before you can remove the domain.
- ◆ Maintenance domains are designed to provide a transparent method of verifying and resolving connectivity problems for end-to-end connections. By default, these connections run between the domain service access points (DSAPs) within each MA defined for a domain, and are manually configured using the `ethernet cfm mep` command.

In contrast, MIPs are interconnection points that make up all possible paths between the DSAPs within an MA. MIPs are automatically generated by the CFM protocol when the `mip-creation` option in this command is set to "default" or "explicit," and the MIP creation state machine is invoked (as defined in IEEE 802.1ag). The default option allows MIPs to be created for all interconnection points within an MA, regardless of the domain's level in the maintenance hierarchy (e.g., customer, provider, or operator). While the explicit option only generates MIPs within an MA if its associated domain is not at the bottom of the maintenance hierarchy. This option is used to hide the structure of network at the lowest domain level.

The diagnostic functions provided by CFM can be used to detect connectivity failures between any pair of MEPs in an MA. Using MIPs allows these failures to be isolated to smaller segments of the network.

Allowing the CFM to generate MIPs exposes more of the network structure to users at higher domain levels, but can speed up the process of fault detection and recovery. This trade-off should be carefully considered when designing a CFM maintenance structure.

Also note that while MEPs are active agents which can initiate consistency check messages (CCMs), transmit loop back or link trace messages, and maintain the local CCM database. MIPs, on the other hand are passive agents



which can only validate received CFM messages, and respond to loop back and link trace messages.

The MIP creation method defined by the `ma index name` command takes precedence over the method defined by this command.

### Example

This example creates a maintenance domain set to maintenance level 3, and enters CFM configuration mode for this domain.

```
Console(config)#ethernet cfm domain index 1 name voip level 3 mip-creation  
explicit  
Console(config-ether-cfm)#
```

### Related Commands

[ma index name \(714\)](#)

**ethernet cfm enable** This command enables CFM processing globally on the switch. Use the **no** form to disable CFM processing globally.

### Syntax

**[no] ethernet cfm enable**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to globally enabling CFM processing with this command. Specifically, the maintenance domains, maintenance associations, and MEPs should be configured on each participating bridge.
- ◆ When CFM is enabled, hardware resources are allocated for CFM processing.

### Example

This example enables CFM globally on the switch.

```
Console(config)#ethernet cfm enable  
Console(config)#
```

**ma index name** This command creates a maintenance association (MA) within the current maintenance domain, maps it to a customer service instance (S-VLAN), and sets the manner in which MIPs are created for this service instance. Use the **no** form with the **vlan** keyword to remove the S-VLAN from the specified MA. Or use the **no** form with only the **index** keyword to remove the MA from the current domain.

### Syntax

**ma index** *index name* *ma-name* [**vlan** *vlan-list* [**mip-creation** *type*]]

**no ma index** *index* [**vlan** *vlan-list*]

*index* – MA identifier. (Range: 1-2147483647)

*ma-name* – MA name. (Range: 1-43 alphanumeric characters)

*vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

*type* – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:

**default** – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.

**explicit** – MIPs can be created this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

**none** – No MIP can be created for this MA.

### Default Setting

10 seconds

### Command Mode

CFM Domain Configuration

### Command Usage

- ◆ The maintenance domain used to enter CFM domain configuration mode, the MA name and VLAN identifier specified by this command, and the DSAPs configured with the [mep crosscheck mpid](#) command create a unique service instance for each customer.
- ◆ If only the MA index and name are entered for this command, the MA will be recorded in the domain database, but will not function. No MEPs can be created until the MA is associated with a service VLAN.
- ◆ Note that multiple domains at the same maintenance level (see the [ethernet cfm domain](#) command) cannot have an MA on the same VLAN. Also, each MA name must be unique within the CFM-managed network.
- ◆ The first VLAN entered in the list by this command is the primary VLAN, and is the VLAN on which all CFM functions are executed.

- ◆ Before removing an MA, first remove all the MEPs configured for it (see the [mep crosscheck mpid](#) command).
- ◆ If the MIP creation method is not defined by this command, the creation method defined by the [ethernet cfm domain](#) command is applied to this MA. For a detailed description of the MIP types, refer to the Command Usage section under the [ethernet cfm domain](#) command.

### Example

This example creates a maintenance association, binds it to VLAN 1, and allows MIPs to be created within this MA using the default method.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1 mip-creation default
Console(config-ether-cfm)#
```

**ma index name-format** This command specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format. Use the **no** form to restore the default setting.

### Syntax

**ma index** *index* **name-format** {**character-string** | **icc-based**}

**no ma index** *index* **name-format**

*index* – MA identifier. (Range: 1-2147483647)

**character-string** – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.

**icc-based** – ITU-T SG13/SG15 Y.1731 defined ICC based format.

### Default Setting

character-string

### Command Mode

CFM Domain Configuration

### Example

This example specifies the name format as character string.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name-format character-string
Console(config-ether-cfm)#
```

**ethernet cfm mep** This command sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages. Use the **no** form to delete a MEP.

### Syntax

**ethernet cfm mep mpid** *mpid* **md** *domain-name* **ma** *ma-name* [**up**]

**no ethernet cfm mep mpid** *mpid* **ma** *ma-name*

*mpid* – Maintenance end point identifier. (Range: 1-8191)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

**up** – Indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the **up** keyword is not included in this command, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.

### Default Setting

No MEPs are configured.  
The MEP faces outward (down).

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured (using the **ethernet cfm domain** command), (2) maintenance association within the domain (using the **ma index name** command), and (3) finally the MEP using this command.
- ◆ An interface may belong to more than one domain. This command can be used to configure an interface as a MEP for different MAs in different domains.
- ◆ To change the MEP's MA or the direction it faces, first delete the MEP, and then create a new one.

### Example

This example sets port 1 as a DSAP for the specified maintenance association.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm mep mpid 1 md voip ma rd
Console(config-if)#
```

**ethernet cfm port-enable** This command enables CFM processing on an interface. Use the **no** form to disable CFM processing on an interface.

#### Syntax

**[no] ethernet cfm port-enable**

#### Default Setting

Enabled

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- ◆ An interface must be enabled before a MEP can be created with the **ethernet cfm mep** command.
- ◆ If a MEP has been configured on an interface with the **ethernet cfm mep** command, it must first be deleted before CFM can be disabled on that interface.
- ◆ When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

#### Example

This example enables CFM on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm port-enable
Console(config-if)#
```

**clear ethernet cfm ais mpid** This command clears AIS defect information for the specified MEP.

#### Syntax

**clear ethernet cfm ais mpid mpid md domain-name ma ma-name**

*mpid* – Maintenance end point identifier. (Range: 1-8191)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

#### Default Setting

None

#### Command Mode

Privileged Exec

### Command Usage

This command can be used to clear AIS defect entries if a MEP does not exit the AIS state when all errors are resolved.

### Example

This example clears AIS defect entries on port 1.

```
Console#clear ethernet cfm ais mpid 1 md voip ma rd
Console(config)#
```

**show ethernet cfm configuration** This command displays CFM configuration settings, including global settings, SNMP traps, and interface settings.

### Syntax

**show ethernet cfm configuration** {**global** | **traps** | **interface** *interface*}

**global** – Displays global settings including CFM global status, cross-check start delay, and link trace parameters.

**traps** – Displays the status of all continuity check and cross-check traps.

*interface* – Displays CFM status for the specified interface.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1-8)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows the global settings for CFM.

```
Console#show ethernet cfm configuration global
CFM Global Status      : Enabled
Crosscheck Start Delay : 10 seconds
Linktrace Cache Status : Enabled
Linktrace Cache Hold Time : 100 minutes
Linktrace Cache Size   : 100 entries
Console#
```

This example shows the configuration status for continuity check and cross-check traps.

```

Console#show ethernet cfm configuration traps
CC MEP Up Trap           :Disabled
CC MEP Down Trap        :Disabled
CC Configure Trap       :Disabled
CC Loop Trap            :Disabled
Cross Check MEP Unknown Trap :Disabled
Cross Check MEP Missing Trap :Disabled
Cross Check MA Up       :Disabled
Console#

```

**Table 147: show ethernet cfm configuration traps - display description**

Field	Description
CC MEP Up Trap	Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database.
CC Mep Down Trap	Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.
CC Configure Trap	Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.
CC Loop Trap	Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.
Cross Check MEP Unknown Trap	A CCM is received from a MEP that has not been configured as a DSAP (see the <a href="#">ethernet cfm mep</a> command), manually configured as a remote MEP (see the <a href="#">mep crosscheck mpid</a> command), nor learned through previous CCM messages.
Cross Check MEP Missing Trap	This device failed to receive three consecutive CCMs from another MEP in the same MA.
Cross Check MA Up	Generates a trap when all remote MEPs belonging to an MA come up.

This example shows the CFM status for port 1.

```

Console#show ethernet cfm configuration interface ethernet 1/1
Ethernet 1/1 CFM Status:Enabled
Console#

```

**show ethernet cfm md** This command displays the configured maintenance domains.

### Syntax

**show ethernet cfm md** [**level** *level*]

*level* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows all configured maintenance domains.

```
Console#show ethernet cfm md
MD Index  MD Name          Level  MIP Creation  Archive Hold Time (m.)
-----  -
          1 rd              0      default              100
Console#
```

**show ethernet cfm ma** This command displays the configured maintenance associations.

### Syntax

**show ethernet cfm ma** [**level** *level*]

*level* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

For a description of the values displayed in the CC Interval field, refer to the [ethernet cfm cc ma interval](#) command.

### Example

This example shows all configured maintenance associations.

```
Console#show ethernet cfm ma
MD Name      MA Index MA Name      Primary VID  CC Interval MIP Creation
-----  -
steve                1 voip              1             4 Default
Console#
```



**show ethernet cfm maintenance-points local** This command displays the maintenance points configured on this device.  
**Syntax**

**show ethernet cfm maintenance-points local**  
{**mep** [**domain** *domain-name* | **interface** *interface* | **level** *level-id*] | **mip** [**domain** *domain-name* | **level** *level-id*]}

**mep** – Displays only local maintenance end points.

**mip** – Displays only local maintenance intermediate points.

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*interface* – Displays CFM status for the specified interface.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1-8)

*port* - Port number. (Range: 1-26/28/52)

**port-channel** *channel-id* (Range: 1-16)

*level-id* – Maintenance level for this domain. (Range: 0-7)

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Command Usage

- ◆ Use the **mep** keyword with this command to display the MEPs configured on this device as DSAPs through the [ethernet cfm mep](#) command.
- ◆ Using the **mip** keyword with this command to display the MIPs generated on this device by the CFM protocol when the mip-creation method is set to either "default" or "explicit" by the [ethernet cfm domain](#) command or the [ma index name](#) command.

#### Example

This example shows all MEPs configured on this device for maintenance domain rd.

```

Console#show ethernet cfm maintenance-points local mep
MPID MD Name          Level Direct VLAN Port      CC Status MAC Address
-----
  1 rd                  0 UP           1 Eth 1/ 1 Enabled 00-12-CF-3A-A8-C0
Console#

```

**show ethernet cfm maintenance-points local detail mep** This command displays detailed CFM information about a local MEP in the continuity check database.

#### Syntax

#### **show ethernet cfm maintenance-points local detail mep**

**[domain *domain-name* | interface *interface* | level *level-id*]**

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*interface* – Displays CFM status for the specified interface.

#### **ethernet *unit/port***

*unit* - Unit identifier. (Range: 1-8)

*port* - Port number. (Range: 1-26/28/52)

#### **port-channel *channel-id*** (Range: 1-16)

*level-id* – Maintenance level for this domain. (Range: 0-7)

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Example

This example shows detailed information about the local MEP on port 1.

```
Console#show ethernet cfm maintenance-points local detail mep interface
ethernet 1/1
MEP Settings:
-----
MPID                : 1
MD Name             : vopu
MA Name             : r&d
MA Name Format       : Character String
Level               : 0
Direction           : Up
Interface           : Eth 1/ 1
CC Status           : Enabled
MAC Address         : 00-E0-0C-00-00-FD
Defect Condition    : No Defect
Received RDI        : False
AIS Status          : Enabled
AIS Period          : 1 seconds
AIS Transmit Level  : Default
Suppress Alarm      : Disabled
Suppressing Alarms  : Disabled

Console#
```

**Table 148: show ethernet cfm maintenance-points local detail mep - display**

Field	Description
MPID	MEP identifier
MD Name	The maintenance domain for this entry.
MA Name	Maintenance association to which this remote MEP belongs
MA Name Format	The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID
Level	Maintenance level of the local maintenance point
Direction	The direction in which the MEP faces on the Bridge port (up or down).
Interface	The port to which this MEP is attached.
CC Status	Shows if the MEP will generate CCM messages.
MAC Address	MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been received or the local MEP record times out, the address will be set to the initial value of all Fs.)
Defect Condition	Shows the defect detected on the MEP.
Received RDI	Receive status of remote defect indication (RDI) messages on the MEP.
AIS Status	Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.
AIS Period	The interval at which AIS information is sent.
AIS Transmit Level	The maintenance level at which AIS information will be sent for the specified MEP.
Suppress Alarm	Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.
Suppressing Alarms	Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.

**show ethernet cfm  
maintenance-points  
remote detail**

This command displays detailed CFM information about a remote MEP in the continuity check database.

**Syntax**

**show ethernet cfm maintenance-points remote detail**

{**mac** *mac-address* | **mpid** *mpid*}  
[**domain** *domain-name* | **level** *level-id* | **ma** *ma-name*]

*mac-address* – MAC address of a remote maintenance point.  
This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*mpid* – Maintenance end point identifier. (Range: 1-8191)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Authorized maintenance level for this domain. (Range: 0-7)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Use the **mpid** keyword with this command to display information about a specific maintenance point, or use the **mac** keyword to display information about all maintenance points that have the specified MAC address.

### Example

This example shows detailed information about the remote MEP designated by MPID 2.

```
Console#show ethernet cfm maintenance-points remote detail mpid 2
MAC Address           : 00-0D-54-FC-A2-73
Domain/Level         : voip / 3
MA Name              : rd
Primary VLAN         : 1
MPID                 : 2
Incoming Port        : Eth 1/ 2
CC Lifetime          : 645 seconds
Age of Last CC Message : 2 seconds
Frame Loss           : 137
CC Packet Statistics : 647/1
Port State           : Up
Interface State      : Up
Crosscheck Status    : Enabled

Console#
```

**Table 149: show ethernet cfm maintenance-points remote detail - display**

Field	Description
MAC Address	MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all Fs.)
Domain/Level	Maintenance domain and level of the remote maintenance point
MA Name	Maintenance association to which this remote MEP belongs
Primary VLAN	VLAN to which this MEP belongs
MPID	MEP identifier
Incoming Port	Port to which this remote MEP is attached.
CC Lifetime	Length of time to hold messages about this MEP in the CCM database
Age of Last CC Message	Length of time the last CCM message about this MEP has been in the CCM database
Frame Loss	Percentage of transmitted frames lost
CC Packet Statistics (received/error)	The number of CCM packets received successfully and those with errors

**Table 149: show ethernet cfm maintenance-points remote detail - display**

Field	Description
Port State	Port states include: Up – The port is functioning normally. Blocked – The port has been blocked by the Spanning Tree Protocol. No port state – Either no CCM has been received, or no port status TLV was received in the last CCM.
Interface State	Interface states include: No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM. Up – The interface is ready to pass packets. Down – The interface cannot pass packets. Testing – The interface is in some test mode. Unknown – The interface status cannot be determined for some reason. Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event. Not Present – Some component of the interface is missing. isLowerLayerDown – The interface is down due to state of the lower layer interfaces.
Crosscheck Status	Shows if crosscheck function has been enabled.

## Continuity Check Operations

**ethernet cfm cc ma interval** This command sets the transmission delay between continuity check messages (CCMs). Use the **no** form to restore the default settings.

### Syntax

**ethernet cfm cc md** *domain-name* **ma** *ma-name* **interval** *interval-level*

**no ethernet cfm cc ma** *ma-name* **interval**

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*interval-level* – The transmission delay between connectivity check messages. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (CCM interval field options: 4 - 1 second, 5 - 10 seconds, 6 - 1 minute, 7 - 10 minutes)

### Default Setting

4 (1 second)

### Command Mode

Global Configuration

### Command Usage

- ◆ CCMs provide a means to discover other MEPs and to detect connectivity failures in an MA. If any MEP fails to receive three consecutive CCMs from any other MEPs in its MA, a connectivity failure is registered. The interval at which

CCMs are issued should therefore be configured to detect connectivity problems in a timely manner, as dictated by the nature and size of the MA.

- ◆ The maintenance of a MIP CCM database by a MIP presents some difficulty for bridges carrying a large number of Service Instances, and for whose MEPs are issuing CCMs at a high frequency. For this reason, slower CCM transmission rates may have to be used.

### Example

This example sets the transmission delay for continuity check messages to level 7 (60 seconds).

```
Console(config)#ethernet cfm cc md voip ma rd interval 7
Console(config)#
```

### Related Commands

[ethernet cfm cc enable \(726\)](#)

**ethernet cfm cc enable** This command enables the transmission of continuity check messages (CCMs) within a specified maintenance association. Use the **no** form to disable the transmission of these messages.

### Syntax

**[no] ethernet cfm cc enable md** *domain-name* **ma** *ma-name*

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ CCMs are multicast periodically by a MEP in order to discover other MEPs in the same MA, and to assure connectivity to all other MEPs/MIPs in the MA.
- ◆ Each CCM received is checked to verify that the MEP identifier field sent in the message does not match its own MEPID, which would indicate a duplicate MEP or network loop. If these error types are not found, the CCM is stored in the MEP's local database until aged out.
- ◆ If a maintenance point fails to receive three consecutive CCMs from any other MEP in the same MA, a connectivity failure is registered.

- ◆ If a maintenance point receives a CCM with an invalid MEPID or MA level or an MA level lower than its own, a failure is registered which indicates a configuration error or cross-connect error (i.e., overlapping MAs).

### Example

This example enables continuity check messages for the specified maintenance association.

```
Console(config)#ethernet cfm cc enable md voip ma rd
Console(config)#
```

**snmp-server enable traps ethernet cfm cc** This command enables SNMP traps for CFM continuity check events. Use the **no** form to disable these traps.

### Syntax

**[no] snmp-server enable traps ethernet cfm cc [config | loop | mep-down | mep-up]**

**config** – Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.

**loop** – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.

**mep-down** – Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.

**mep-up** – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which has an expired entry in the archived database.

### Default Setting

All continuity checks are enabled.

### Command Mode

Global Configuration

### Command Usage

All mep-up traps are suppressed when cross-checking of MEPs is enabled because cross-check traps include more detailed status information.

### Example

This example enables SNMP traps for mep-up events.

```
Console(config)#snmp-server enable traps ethernet cfm cc mep-up
Console(config)#
```

### Related Commands

[ethernet cfm mep crosscheck \(733\)](#)

**mep archive-hold-time** This command sets the time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. Use the **no** form to restore the default setting.

### Syntax

**mep archive-hold-time** *hold-time*

*hold-time* – The time to retain data for a missing MEP.  
(Range: 1-65535 minutes)

### Default Setting

100 minutes

### Command Mode

CFM Domain Configuration

### Command Usage

A change to the hold time only applies to entries stored in the database after this command is entered.

### Example

This example sets the aging time for missing MEPs in the CCM database to 30 minutes.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep archive-hold-time 30
Console(config-ether-cfm)#
```

**clear ethernet cfm maintenance-points remote** This command clears the contents of the continuity check database.

### Syntax

**clear ethernet cfm maintenance-points remote** [**domain** *domain-name* | **level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Maintenance level. (Range: 0-7)



### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Use this command without any keywords to clear all entries in the CCM database. Use the **domain** keyword to clear the CCM database for a specific domain, or the **level** keyword to clear it for a specific maintenance level.

### Example

```
Console#clear ethernet cfm maintenance-points remote domain voip  
Console#
```

**clear ethernet cfm errors** This command clears continuity check errors logged for the specified maintenance domain or maintenance level.

### Syntax

**clear ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Use this command without any keywords to clear all entries in the error database. Use the **domain** keyword to clear the error database for a specific domain, or the **level** keyword to clear it for a specific maintenance level.

### Example

```
Console#clear ethernet cfm errors domain voip  
Console#
```

**show ethernet cfm errors** This command displays the CFM continuity check errors logged on this device.

**Syntax**

**show ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Authorized maintenance level for this domain. (Range: 0-7)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```

Console#show ethernet cfm errors
Level VLAN MPID Interface Remote MAC Reason MA Name
-----
5 2 40 Eth 1/1 ab.2f.9c.00.05.01 LEAK provider_1_2
Console#
    
```

**Table 150: show ethernet cfm errors - display description**

Field	Description
Level	Maintenance level associated with this entry.
VLAN	VLAN in which this error occurred.
MPID	Identifier of remote MEP.
Interface	Port at which the error was recorded
Remote MAC	MAC address of remote MEP.
Reason	<p>Error types include:</p> <p>LEAK – MA x is associated with a specific VID list*, one or more of the VIDs in this MA can pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA y, at a higher maintenance level, and associated with at least one of the VID(s) also in MA x, does have a MEP configured on the bridge port.</p> <p>VIDS – MA x is associated with a specific VID list* on this MA on the bridge port, and some other MA y, associated with at least one of the VID(s) also in MA x, also has an Up MEP configured facing inward (up) on some bridge port.</p> <p>EXCESS_LEV – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.</p> <p>OVERLAP_LEV – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities.</p>
MA	The maintenance association for this entry.

\* This definition is based on the IEEE 802.1ag standard. Current software for this switch only supports a single VLAN per MA. However, since it may interact with other devices which support multiple VLAN assignments per MA, this error message may be reported.

## Cross Check Operations

**ethernet cfm mep crosscheck start-delay** This command sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm mep crosscheck start-delay** *delay*

*delay* – The time a device waits for remote MEPs to come up before the cross-check is started. (Range: 1-65535 seconds)

### Default Setting

30 seconds

### Command Mode

Global Configuration

### Command Usage

- ◆ This command sets the delay that a device waits for a remote MEP to come up, and it starts cross-checking the list of statically configure remote MEPs in the local maintenance domain against the MEPs learned through CCMs.
- ◆ The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps.

### Example

This example sets the maximum delay before starting the cross-check process.

```
Console(config)#ethernet cfm mep crosscheck start-delay 60
Console(config)#
```

**snmp-server enable traps ethernet cfm crosscheck** This command enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages (CCMs). Use the **no** form to restore disable these traps.

### Syntax

**[no] snmp-server enable traps ethernet cfm crosscheck [ma-up | mep-missing | mep-unknown]**

**ma-up** – Sends a trap when all remote MEPs in an MA come up.

**mep-missing** – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list.

**mep-unknown** – Sends a trap if an unconfigured MEP comes up.

### Default Setting

All continuity checks are enabled.

### Command Mode

Global Configuration

### Command Usage

- ◆ For this trap type to function, cross-checking must be enabled on the required maintenance associations using the `ethernet cfm mep crosscheck` command.
- ◆ A mep-missing trap is sent if cross-checking is enabled (with the `ethernet cfm mep crosscheck` command), and no CCM is received for a remote MEP configured in the static list (with the `mep crosscheck mpid` command).
- ◆ A mep-unknown trap is sent if cross-checking is enabled, and a CCM is received from a remote MEP that is not configured in the static list.
- ◆ A ma-up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association.

### Example

This example enables SNMP traps for mep-unknown events detected in cross-check operations.

```
Console(config)#snmp-server enable traps ethernet cfm crosscheck mep-unknown  
Console(config)#
```

**mep crosscheck mpid** This command statically defines a remote MEP in a maintenance association. Use the **no** form to remove a remote MEP.

### Syntax

**[no] mep crosscheck mpid mpid ma ma-name**

*mpid* – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

No remote MEPs are configured.

### Command Mode

CFM Domain Configuration

### Command Usage

- ◆ Use this command to statically configure remote MEPs that exist inside the maintenance association. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.
- ◆ Remote MEPs can only be configured with this command if domain service access points (DSAPs) have already been created with the `ethernet cfm mep` command at the same maintenance level and in the same MA. DSAPs are MEPs that exist on the edge of the domain, and act as primary service access points for end-to-end cross-check, loop-back, and link-trace functions.

### Example

This example defines a static MEP for the specified maintenance association.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1
Console(config-ether-cfm)#mep crosscheck mpid 2 ma rd
Console(config-ether-cfm)#
```

### ethernet cfm mep crosscheck

This command enables cross-checking between the static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through continuity check messages (CCMs). Use the **disable** keyword to stop the cross-check process.

### Syntax

```
ethernet cfm mep crosscheck {enable | disable} md domain-name  
ma ma-name
```

**enable** – Starts the cross-check process.

**disable** – Stops the cross-check process.

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – MA name. (Range: 1-43 alphanumeric characters)

### Default Setting

Disabled

### Command Mode

Privileged Exec

### Command Usage

- ◆ Before using this command to start the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the `mep crosscheck mpid` command. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.

- ◆ The cross-check process is disabled by default, and must be manually started using this command with the **enable** keyword.

### Example

This example enables cross-checking within the specified maintenance association.

```
Console#ethernet cfm mep crosscheck enable md voip ma rd
Console#
```

### show ethernet cfm maintenance-points remote crosscheck

This command displays information about remote MEPs statically configured in a cross-check list.

### Syntax

#### show ethernet cfm maintenance-points remote crosscheck

[**domain** *domain-name* | **mpid** *mpid*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*mpid* – Maintenance end point identifier. (Range: 1-8191)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows all remote MEPs statically configured on this device.

```
Console#show ethernet cfm maintenance-points remote crosscheck
MPID  MA Name                Level  VLAN  MEP Up  Remote MAC
-----
  2   downtown                4      2   Yes    00-0D-54-FC-A2-73
Console#
```

## Link Trace Operations

### ethernet cfm linktrace cache

This command enables caching of CFM data learned through link trace messages. Use the **no** form to disable caching.

### Syntax

[**no**] **ethernet cfm linktrace cache**

### Default Setting

Enabled

### Command Mode

Global Configuration

### Command Usage

- ◆ A link trace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the link trace message reaches its destination or can no longer be forwarded.
- ◆ Use this command to enable the link trace cache to store the results of link trace operations initiated on this device. Use the [ethernet cfm linktrace](#) command to transmit a link trace message.
- ◆ Link trace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.

### Example

This example enables link trace caching.

```
Console(config)#ethernet cfm linktrace cache
Console(config)#
```

**ethernet cfm linktrace cache hold-time** This command sets the hold time for CFM link trace cache entries. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm linktrace cache hold-time** *minutes*

*minutes* – The aging time for entries stored in the link trace cache.  
(Range: 1-65535 minutes)

### Default Setting

100 minutes

### Command Mode

Global Configuration

### Command Usage

Before setting the aging time for cache entries, the cache must first be enabled with the [ethernet cfm linktrace cache](#) command.

### Example

This example sets the aging time for entries in the link trace cache to 60 minutes.

```
Console(config)#ethernet cfm linktrace cache hold-time 60
Console(config)#
```

**ethernet cfm linktrace cache size** This command sets the maximum size for the link trace cache. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm linktrace cache size** *entries*

*entries* – The number of link trace responses stored in the link trace cache.  
(Range: 1-4095 entries)

### Default Setting

100 entries

### Command Mode

Global Configuration

### Command Usage

- ◆ Before setting the cache size, the cache must first be enabled with the [ethernet cfm linktrace cache](#) command.
- ◆ If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased with this command, or purged with the [clear ethernet cfm linktrace-cache](#) command.

### Example

This example limits the maximum size of the link trace cache to 500 entries.

```
Console(config)#ethernet cfm linktrace cache size 500
Console(config)#
```

**ethernet cfm linktrace** This command sends CFM link trace messages to the MAC address of a remote MEP.

### Syntax

**ethernet cfm linktrace** {**dest-mep** *destination-mpid* | **src-mep** *source-mpid* | **dest-mep** *destination-mpid* | *mac-address*} | *mac-address*} **md** *domain-name* **ma** *ma-name* [**tll** *number*]

*destination-mpid* – The identifier of a remote MEP that is the target of the link trace message. (Range: 1-8191)



*source-mpid* – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)

*mac-address* – MAC address of a remote MEP that is the target of the link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*number* – The time to live of the linktrace message. (Range: 0-255 hops)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

- ◆ Link trace messages can be targeted to MEPs, not MIPs. Before sending a link trace message, be sure you have configured the target MEP for the specified MA.
- ◆ If the MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the [show ethernet cfm maintenance-points remote crosscheck](#) command to verify that a MAC address has been learned for the target MEP.
- ◆ Link trace messages (LTMs) are sent as multicast CFM frames, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the LTM reaches its destination or can no longer be forwarded.
- ◆ Link trace messages are used to isolate faults. However, this task can be difficult in an Ethernet environment, since each node is connected through multipoint links. Fault isolation is even more challenging since the MAC address of the target node can age out in several minutes. This can cause the traced path to vary over time, or connectivity lost if faults cause the target MEP to be isolated from other MEPs in an MA.
- ◆ When using the command line or web interface, the source MEP used by to send a link trace message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

### Example

This example sends a link trace message to the specified MEP with a maximum hop count of 25.

```
Console#linktrace ethernet dest-mep 2 md voip ma rd ttl 25
Console#
```

**clear ethernet cfm linktrace-cache** This command clears link trace messages logged on this device.

**Command Mode**  
Privileged Exec

**Example**

```
Console#clear ethernet cfm linktrace-cache
Console#
```

**show ethernet cfm linktrace-cache** This command displays the contents of the link trace cache.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ethernet cfm linktrace-cache
Hops MA                IP / Alias          Ingress MAC          Ing. Action Relay
                Forwarded          Egress MAC           Egr. Action
-----
   2 rd                192.168.0.6        00-12-CF-12-12-2D  ingOk              Hit
                Not Forwarded
Console#
```

**Table 151: show ethernet cfm linktrace-cache - display description**

Field	Description
Hops	The number hops taken to reach the target MEP.
MA	Name of the MA to which this device belongs.
IP/Alias	IP address or alias of the target device's CPU.
Forwarded	Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP.
Ingress MAC	MAC address of the ingress port on the target device.
Egress MAC	MAC address of the egress port on the target device.
Ing. Action	Action taken on the ingress port: IngOk – The target data frame passed through to the MAC Relay Entity. IngDown – The bridge port's MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port's MAC_Operational parameter to be false. IngBlocked – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state. IngVid – The ingress port is not in the member set of the LTM's VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering.

**Table 151: show ethernet cfm linktrace-cache - display description** (Continued)

Field	Description
Egr. Action	Action taken on the egress port: EgrOk – The targeted data frame was forwarded. EgrDown – The Egress Port can be identified, but that bridge port’s MAC_Operational parameter is false. EgrBlocked – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in the forwarding state. EgrVid – The Egress Port can be identified, but the bridge port is not in the LTM’s VID member set, and was therefore filtered by egress filtering.
Relay	Relay action: FDB – Target address found in forwarding database. MPDB – Target address found in the maintenance point database. HIT – Target located on this device.

## Loopback Operations

**ethernet cfm loopback** This command sends CFM loopback messages to a MAC address for a MEP or MIP.

### Syntax

**ethernet cfm loopback** {**dest-mep** *destination-mpid* | **src-mep** *source-mpid* {**dest-mep** *destination-mpid* | *mac-address*} | *mac-address*} **md** *domain-name* **ma** *ma-name* [**count** *transmit-count*] [**size** *packet-size*]

*destination-mpid* – The identifier of a MEP that is the target of the loopback message. (Range: 1-8191)

*source-mpid* – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)

*mac-address* – MAC address of the remote maintenance point that is the target of the loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*transmit-count* – The number of times the loopback message is sent. (Range: 1-1024)

*packet-size* – The size of the loopback message. (Range: 64-1518 bytes)

### Default Setting

Loop back count: One loopback message is sent.

Loop back size: 64 bytes

### Command Mode

Privileged Exec

### Command Usage

- ◆ Use this command to test the connectivity between maintenance points. If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.
- ◆ The point from which the loopback message is transmitted (i.e., the DSAP) and the target maintenance point specified in this command must be within the same MA.
- ◆ Loop back messages can be used for fault verification and isolation after automatic detection of a fault or receipt of some other error report. Loopback messages can also be used to confirm the successful restoration or initiation of connectivity. The receiving maintenance point should respond to the loop back message with a loopback reply.
- ◆ When using the command line or web interface, the source MEP used by to send a loopback message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

### Example

This example sends a loopback message to the specified remote MEP.

```
Console#ethernet cfm loopback dest-mep 1 md voip ma rd  
Console#
```

## Fault Generator Operations

**mep fault-notify alarm-time** This command sets the time a defect must exist before a fault alarm is issued. Use the **no** form to restore the default setting.

### Syntax

**mep fault-notify alarm-time** *alarm-time*

**no fault-notify alarm-time**

*alarm-time* – The time that one or more defects must be present before a fault alarm is generated. (Range: 3-10 seconds)

### Default Setting

3 seconds

### Command Mode

CFM Domain Configuration

### Command Usage

A fault alarm is issued when the MEP fault notification generator state machine detects that a time period configured by this command has passed with one or

more defects indicated, and fault alarms are enabled at or above the priority level set by the [mep fault-notify lowest-priority](#) command.

### Example

This example set the delay time before generating a fault alarm.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify alarm-time 10
Console(config-ether-cfm)#
```

**mep fault-notify lowest-priority** This command sets the lowest priority defect that is allowed to generate a fault alarm. Use the **no** form to restore the default setting.

### Syntax

**mep fault-notify lowest-priority** *priority*

**no fault-notify lowest-priority**

*priority* – Lowest priority default allowed to generate a fault alarm.  
(Range: 1-6)

### Default Setting

Priority level 2

### Command Mode

CFM Domain Configuration

### Command Usage

- ◆ A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that a configured time period (see the [mep fault-notify alarm-time](#) command) has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by this command. The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (see the [mep fault-notify reset-time](#) command) without a defect indication. The normal procedure upon receiving a fault alarm is to inspect the reporting MEP's managed objects using an appropriate SNMP software tool, diagnose the fault, correct it, re-examine the MEP's managed objects to see whether the MEP fault notification generator state machine has been reset, and repeat those steps until the fault is resolved.
- ◆ Only the highest priority defect currently detected is reported in the fault alarm.

- ◆ Priority defects include the following items:

**Table 152: Remote MEP Priority Levels**

Priority Level	Level Name	Description
1	allDef	All defects.
2	macRemErrXcon	DefMACstatus, DefRemoteCCM, DefErrorCCM, or DefXconCCM.
3	remErrXcon	DefErrorCCM, DefXconCCM or DefRemoteCCM.
4	errXcon	DefErrorCCM or DefXconCCM.
5	xcon	DefXconCCM
6	noXcon	No defects DefXconCCM or lower are to be reported.

**Table 153: MEP Defect Descriptions**

Field	Description
DefMACstatus	Either some remote MEP is reporting its Interface Status TLV as not isUp, or all remote MEPs are reporting a Port Status TLV that contains some value other than psUp.
DefRemoteCCM	The MEP is not receiving valid CCMs from at least one of the remote MEPs.
DefErrorCCM	The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.
DefXconCCM	The MEP has received at least one CCM from either another MAID or a lower MD Level whose CCM Interval has not yet timed out.

### Example

This example sets the lowest priority defect that will generate a fault alarm.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify lowest-priority 1
Console(config-ether-cfm)#
```

### mep fault-notify reset-time

This command configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. Use the **no** form to restore the default setting.

### Syntax

**mep fault-notify reset-time** *reset-time*

**no fault-notify reset-time**

*reset-time* – The time that must pass without any further defects indicated before another fault alarm can be generated. (Range: 3-10 seconds)

### Default Setting

10 seconds

### Command Mode

CFM Domain Configuration

### Example

This example sets the reset time after which another fault alarm can be generated.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify reset-time 7
Console(config-ether-cfm)#
```

### show ethernet cfm fault-notify-generator

This command displays configuration settings for the fault notification generator.

### Syntax

**show ethernet cfm fault-notify-generator mep *mpid***

*mpid* – Maintenance end point identifier. (Range: 1-8191)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows the fault notification settings configured for one MEP.

```
Console#show ethernet cfm fault-notify-generator mep 1
MD Name      MA Name      Highest Defect Lowest Alarm  Alarm Time Reset Time
-----
      voip      rd none      macRemErrXcon  3sec.    10sec.
Console#
```

**Table 154: show fault-notify-generator - display description**

Field	Description
MD Name	The maintenance domain for this entry.
MA Name	The maintenance association for this entry.
Hihest Defect	The highest defect that will generate a fault alarm. (This is disabled by default.)
Lowest Alarm	The lowest defect that will generate a fault alarm (see the <a href="#">mep fault-notify lowest-priority</a> command).

**Table 154: show fault-notify-generator - display description** (Continued)

Field	Description
Alarm Time	The time a defect must exist before a fault alarm is issued (see the <a href="#">mep fault-notify alarm-time</a> command).
Reset Time	The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued (see the <a href="#">mep fault-notify reset-time</a> command).

## Delay Measure Operations

**ethernet cfm delay-measure two-way** This command sends periodic delay-measure requests to a specified MEP within a maintenance association.

### Syntax

**ethernet cfm delay-measure two-way** [**src-mep** *source-mpid*] {**dest-mep** *destination-mpid* | *mac-address*} **md** *domain-name* **ma** *ma-name* [**count** *transmit-count*] [**interval** *interval*] [**size** *packet-size*] [**timeout** *timeout*]

*source-mpid* – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)

*destination-mpid* – The identifier of a remote MEP that is the target of the delay-measure message. (Range: 1-8191)

*mac-address* – MAC address of a remote MEP that is the target of the delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*count* – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5)

*interval* – The transmission delay between delay-measure messages. (Range: 1-5 seconds)

*packet-size* – The size of the delay-measure message. (Range: 64-1518 bytes)

*timeout* – The timeout to wait for a response. (Range: 1-5 seconds)

### Default Setting

Count: 5  
Interval: 1 second  
Size: 64 bytes  
Timeout: 5 seconds

### Command Mode

Privileged Exec



### Command Usage

- ◆ Delay measurement can be used to measure frame delay and frame delay variation between MEPs.
- ◆ A local MEP must be configured for the same MA before you can use this command.
- ◆ If a MEP is enabled to generate frames with delay measurement (DM) information, it periodically sends DM frames to its peer MEP in the same MA., and expects to receive DM frames back from it.
- ◆ Frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with DM request information with the TxTimeStampf (Timestamp at the time of sending a frame with DM request information), and the receiving MEP responds with a frame with DM reply information with TxTimeStampf copied from the DM request information, RxTimeStampf (Timestamp at the time of receiving a frame with DM request information), and TxTimeStamptb (Timestamp at the time of transmitting a frame with DM reply information):
 
$$\text{Frame Delay} = (\text{RxTimeStampb} - \text{TxTimeStampf}) - (\text{TxTimeStamptb} - \text{RxTimeStampf})$$
- ◆ The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

### Example

This example sends periodic delay-measure requests to a remote MEP.

```

Console#ethernet cfm delay-measure two-way dest-mep 1 md voip ma rd
Type ESC to abort.
Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.
Sequence  Delay Time (ms.)  Delay Variation (ms.)
-----  -
          1                < 10                0
          2                < 10                0
          3                < 10                0
          4                 40                40
          5                < 10                40
Success rate is 100% (5/5), delay time min/avg/max=0/8/40 ms.
Average frame delay variation is 16 ms.
Console#
  
```



## OAM Commands

The switch provides OAM (Operation, Administration, and Maintenance) remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loop back testing, and displaying device information.

**Table 155: OAM Commands**

Command	Function	Mode
<code>efm oam</code>	Enables OAM services	IC
<code>efm oam critical-link-event</code>	Enables reporting of critical event or dying gasp	IC
<code>efm oam link-monitor frame</code>	Enables reporting of errored frame link events	IC
<code>efm oam link-monitor frame threshold</code>	Sets the threshold for errored frame link events	IC
<code>efm oam link-monitor frame window</code>	Sets the monitor period for errored frame link events	IC
<code>efm oam mode</code>	Sets the OAM operational mode to active or passive	IC
<code>clear efm oam counters</code>	Clears statistical counters for various OAMPDU message types	PE
<code>clear efm oam event-log</code>	Clears all entries from the OAM event log for the specified port	PE
<code>efm oam remote-loopback</code>	Initiates or terminates remote loopback test	PE
<code>efm oam remote-loopback test</code>	Performs remote loopback test, sending a specified number of packets	PE
<code>show efm oam counters interface</code>	Displays counters for various OAM PDU message types	NE,PE
<code>show efm oam event-log interface</code>	Displays OAM event log	NE,PE
<code>show efm oam remote-loopback interface</code>	Displays results of OAM remote loopback test	NE,PE
<code>show efm oam status interface</code>	Displays OAM configuration settings and event counters	NE,PE
<code>show efm oam status remote interface</code>	Displays information about attached OAM-enabled devices	NE,PE

**efm oam** This command enables OAM functions on the specified port. Use the **no** form to disable this function.

### Syntax

**[no] efm oam**

### Default Setting

Disabled

### Command Mode

Interface Configuration

### Command Usage

- ◆ If the remote device also supports OAM, both exchange Information OAMPDUs to establish an OAM link.
- ◆ Not all CPEs support OAM functions, and OAM is therefore disabled by default. If the CPE attached to a port supports OAM, then this functionality must first be enabled by the **efm oam** command to gain access to other remote configuration functions.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam
Console(config-if)#
```

**efm oam critical-link-event** This command enables reporting of critical event or dying gasp. Use the **no** form to disable this function.

### Syntax

**[no] efm oam critical-link-event {critical-event | dying-gasp}**

**critical-event** - If a critical event occurs, the local OAM entity (this switch) indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log.

**dying-gasp** - If an unrecoverable condition occurs, the local OAM entity indicates this by immediately sending a trap message.

### Default Setting

Enabled

### Command Mode

Interface Configuration

### Command Usage

- ◆ Critical events are vendor-specific and may include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.
- ◆ Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.



**Note:** When system power fails, the switch will always send a dying gasp trap message prior to power down.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam critical-link-event dying-gasp
Console(config-if)#
```

### efm oam link-monitor frame

This command enables reporting of errored frame link events. Use the **no** form to disable this function.

### Syntax

**[no] efm oam link-monitor frame**

### Default Setting

Enabled

### Command Mode

Interface Configuration

### Command Usage

- ◆ An errored frame is a frame in which one or more bits are errored.
- ◆ If this feature is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame
Console(config-if)#
```

**efm oam link-monitor frame threshold** This command sets the threshold for errored frame link events. Use the **no** form to restore the default setting.

#### Syntax

**efm oam link-monitor frame threshold** *count*

**no efm oam link-monitor frame threshold**

*count* - The threshold for errored frame link events. (Range: 1-65535)

#### Default Setting

1

#### Command Mode

Interface Configuration

#### Command Usage

If this feature is enabled, an event notification message is sent if the threshold is reached or exceeded within the period specified by the [efm oam link-monitor frame window](#) command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

#### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame threshold 5
Console(config-if)#
```

**efm oam link-monitor frame window** This command sets the monitor period for errored frame link events. Use the **no** form to restore the default setting.

#### Syntax

**efm oam link-monitor frame window** *size*

**no efm oam link-monitor frame window**

*size* - The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 units of 10 milliseconds)

#### Default Setting

10 (units of 100 milliseconds) = 1 second

#### Command Mode

Interface Configuration

#### Command Usage

If this feature is enabled, an event notification message is sent if the threshold specified by the [efm oam link-monitor frame threshold](#) command is reached or

exceeded within the period specified by this command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

### Example

This example set the window size to 5 seconds.

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame window 50
Console(config-if)#
```

**efm oam mode** This command sets the OAM mode on the specified port. Use the **no** form to restore the default setting.

### Syntax

**efm oam mode** {**active** | **passive**}

**no efm oam mode**

**active** - All OAM functions are enabled.

**passive** - All OAM functions are enabled, except for OAM discovery, and sending loopback control OAMPDUs.

### Default Setting

Active

### Command Mode

Interface Configuration

### Command Usage

When set to active mode, the selected interface will initiate the OAM discovery process. When in passive mode, it can only respond to discovery messages.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam mode active
Console(config-if)#
```

**clear efm oam counters** This command clears statistical counters for various OAMPDU message types.

#### Syntax

**clear efm oam counters** [*interface-list*]

*interface-list* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

#### Command Mode

Privileged Exec

#### Example

```
Console#clear efm oam counters
Console#
```

#### Related Commands

[show efm oam counters interface \(755\)](#)

**clear efm oam event-log** This command clears all entries from the OAM event log for the specified port.

#### Syntax

**clear efm oam event-log** [*interface-list*]

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

#### Command Mode

Privileged Exec

#### Example

```
Console#clear efm oam event-log
Console#
```



**efm oam remote-loopback** This command starts or stops OAM loopback test mode to the attached CPE.

#### Syntax

**efm oam remote-loopback** {**start** | **stop**} *interface*

**start** - Starts remote loopback test mode.

**stop** - Stops remote loopback test mode.

*interface* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Command Usage

- ◆ OAM remote loop back can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loop back testing.
- ◆ Use the **efm oam remote-loopback start** command to start OAM remote loop back test mode on the specified port. Afterwards, use the **efm oam remote-loopback test** command to start sending test packets. Then use the **efm oam remote loopback stop** command to terminate testing (if test packets are still being sent) and to terminate loop back test mode.
- ◆ The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode.
- ◆ During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.
- ◆ During loopback testing, both the switch and remote device are permitted to send OAMPDUs to the peer device and to process any OAMPDUs received from the peer.

#### Example

```
Console#efm oam remote-loopback start 1/1
Loopback operation is processing, please wait.
Enter loopback mode succeeded.
Console#
```

**efm oam remote-loopback test** This command performs a remote loopback test, sending a specified number of packets.

### Syntax

**efm oam remote-loopback test** *interface* [*number-of-packets* [*packet-size*]]

*interface* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-26/28/52)

*number-of-packets* - Number of packets to send. (Range: 1-99999999)

*packet-size* - Size of packets to send. (Range: 64-1518 bytes)

### Default Setting

Number of packets: 10,000

Packet size: 64 bytes

### Command Mode

Privileged Exec

### Command Usage

- ◆ You can use this command to perform an OAM remote loopback test on the specified port. The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode.
- ◆ During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.
- ◆ OAM remote loopback can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loopback testing.
- ◆ A summary of the test is displayed after it is finished.

### Example

```

Console#efm oam remote-loopback test 1/1
Loopback test is processing, press ESC to suspend.
....
Port OAM loopback Tx OAM loopback Rx Loss Rate
-----
1/2          1990          1016    48.94 %
Console#

```

**show efm oam counters interface** This command displays counters for various OAM PDU message types.

#### Syntax

**show efm oam counters interface** [*interface-list*]

*interface-list* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

#### Command Mode

Normal Exec, Privileged Exec

#### Example

```

Console#show efm oam counters interface 1/1
Port OAMPDU Type          TX          RX
-----
1/1  Information            1121        1444
1/1  Event Notification      0           0
1/1  Loopback Control        1           0
1/1  Organization Specific  76          0
Console#

```

**show efm oam event-log interface** This command displays the OAM event log for the specified port(s) or for all ports that have logs.

**show efm oam event-log interface** [*interface-list*]

*interface-list* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

#### Command Mode

Normal Exec, Privileged Exec

#### Command Usage

- ◆ When a link event occurs, no matter whether the location is local or remote, this information is entered in the OAM event log.
- ◆ When the log system becomes full, older events are automatically deleted to make room for new entries.

**Example**

```

Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 00:24:07 2001/01/01
  "Unit 1, Port 1: Dying Gasp at Remote"
Console#

```

This command can show OAM link status changes for link partner as shown in this example.

```

Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 10:22:55 2013/09/13
  "Unit 1, Port 1: Connection to remote device is up at Local"
 10:22:44 2013/09/13
  "Unit 1, Port 1: Connection to remote device is down at Local"
  <--- When the link is down, this event will be written to OAM event-log
 10:20:02 2013/09/13
  "Unit 1, Port 1: Connection to remote device is up at Local"
  <--- When the link is up, this event will be written to OAM event-log,
Console#clear efm oam event-log
  <--- Use the "clear efm oam event-log" command to clear the event-log.
Console#show efm oam event-log interface 1/1
Console#

```

This command can show OAM dying gasp changes for link partner as shown in this example.

```

Console#show efm oam event-log interface 1/1
  <--- When dying gasp happens and the switch get these packets, it will log
  this event in OAM event-log.
OAM event log of Eth 1/1:
 10:27:21 2013/09/13
  "Unit 1, Port 1: Connection to remote device is down at Local"
 10:27:20 2013/09/13
  "Unit 1, Port 1: Dying Gasp occurred at Remote"
Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 10:28:31 2013/09/13
  "Unit 1, Port 1: Connection to remote device is up at Local"
 10:28:28 2013/09/13
  "Unit 1, Port 1: Dying Gasp clear occurred at Remote"
  <--- When the remote device comes up, the switch will get OAM packets
  without the dying gasp bit and display "dying gasp event clear".
Console#

```

**show efm oam remote-loopback interface** This command displays the results of an OAM remote loopback test.  
**Syntax**

**show efm oam remote-loopback interface** [*interface-list*]

*interface-list* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

### Command Mode

Normal Exec, Privileged Exec

### Example

```

Console#show efm oam remote-loopback interface 1/1
Port OAM loopback Tx OAM loopback Rx Loss Rate
-----
1/1                2300                2250        0.01 %
Console#

```

**show efm oam status interface** This command displays OAM configuration settings and event counters.

### Syntax

**show efm oam status interface** [*interface-list*] [**brief**]

*interface* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

**brief** - Displays a brief list of OAM configuration states.

### Command Mode

Normal Exec, Privileged Exec

### Example

```

Console#show efm oam status interface 1/1
OAM information of Eth 1/1:
Basic Information:
Admin State                : Enabled
Operation State            : Operational
Mode                        : Active
Remote Loopback            : Disabled
Remote Loopback Status    : No loopback
Dying Gasp                 : Enabled
Critical Event             : Enabled

```

```

Link Monitor (Errored Frame) : Enabled
Link Monitor:
  Errored Frame Window (100msec) : 10
  Errored Frame Threshold : 1
Console#show efm oam status interface 1/1 brief
$ = local OAM in loopback
* = remote OAM in loopback

Port Admin   Mode      Remote   Dying   Critical Errored
  State      Loopback Gasp     Event   Frame
-----
1/1  Enabled Active  Disabled Enabled Enabled  Enabled
Console#

```

**show efm oam status remote interface** This command displays information about attached OAM-enabled devices.

### Syntax

**show efm oam status remote interface** [*interface-list*]

*interface-list* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-26/28/52)

### Command Mode

Normal Exec, Privileged Exec

### Example

```

Console#show efm oam status remote interface 1/1
Port MAC Address      OUI      Remote   Unidirectional Link   MIB Variable
  Loopback            Retrieval
-----
1/1  00-12-CF-6A-07-F6  000084  Enabled  Disabled      Enabled Disabled
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 156: 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 \(762\)](#)



**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 \(762\)](#)

[ip name-server \(763\)](#)

**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 \(760\)](#)

[ip name-server \(763\)](#)

[ip domain-lookup \(761\)](#)

**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          rd5
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
  10.1.1.0.55
Console#
```

### Related Commands

[ip domain-name \(762\)](#)

[ip domain-lookup \(761\)](#)

**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
  1   2  Address  2001:DB8:1::12
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 157: 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 158: 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**

Disabled

**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

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 159: DHCP Commands**

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IP address information
DHCP Relay	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 160: 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 duid</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 62.

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 = "Edge-core";
# 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 161: 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 162: 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 \(773\)](#)

**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): ECS4510-28T
  DHCP Relay Server:
Console#
```

#### Related Commands

[ip address \(782\)](#)

**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 \(795\)](#)

**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 \(794\)](#)

## DHCP Relay

This section describes commands used to configure the switch to relay DHCP requests from local hosts to a remote DHCP server.

**Table 163: DHCP Relay Option 82 Commands**

Command	Function	Mode
<i>DHCP Relay for IPv4</i>		
<a href="#">ip dhcp relay server</a>	Specifies DHCP server or relay server addresses	IC
<a href="#">ip dhcp restart relay</a>	Enables DHCP relay agent	PE

**ip dhcp relay server** This command specifies the DHCP server or relay server addresses to use. Use the **no** form to clear all addresses.

**Syntax**

**ip dhcp relay server** *address1* [*address2* [*address3* ...]]

**no ip dhcp relay server**

*address* - IP address of DHCP server. (Range: 1-5 addresses)

**Default Setting**

None

**Command Mode**

Interface Configuration (VLAN)

**Usage Guidelines**

- ◆ DHCP relay service 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

```
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 \(778\)](#)

**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 sees 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): ECS4510-28T
  DHCP Relay Server:
Console#
```

### Related Commands

[ip dhcp relay server \(777\)](#)



# 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 164: IP Interface Commands**

Command Group	Function
<a href="#">IPv4 Interface</a>	Configures an IPv4 address for the switch
<a href="#">IPv6 Interface</a>	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 165: IPv4 Interface Commands**

Command Group	Function
<a href="#">Basic IPv4 Configuration</a>	Configures the IP address for interfaces and the gateway router
<a href="#">ARP Configuration</a>	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 166: Basic IP Configuration Commands**

Command	Function	Mode
<a href="#">ip address</a>	Sets the IP address for the current interface	IC
<a href="#">ip default-gateway</a>	Defines the default gateway through which this switch can reach other subnetworks	GC
<a href="#">show ip default-gateway</a>	Displays the default gateway configured for this device	PE
<a href="#">show ip interface</a>	Displays the IP settings for this device	PE
<a href="#">show ip route</a>	Displays specified entries in the routing table	PE
<a href="#">show ip traffic</a>	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
<a href="#">traceroute</a>	Shows the route packets take to the specified host	PE
<a href="#">ping</a>	Sends ICMP echo request packets to another node on the network	NE, 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 \(773\)](#)

[ip default-gateway \(784\)](#)

[ipv6 address \(794\)](#)

**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 \(782\)](#)

[ip route \(816\)](#)

[ipv6 default-gateway \(793\)](#)



**show ip default-gateway** This command shows the IPv4 default gateway configured for this device.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```
Console#show ip default-gateway
IP default gateway 10.1.0.254
Console#
```

**Related Commands**

[ip default-gateway \(784\)](#)

[show ipv6 default-gateway \(802\)](#)

**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): ECS4510-28T
Console#
```

**Related Commands**

[ip address \(782\)](#)

[show ipv6 interface \(802\)](#)

**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 763) and host name-to-address translation enabled (page 761). If necessary, local devices can also be specified in the DNS static host table (page 762).

### 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 \(372\)](#)

**ARP Configuration** This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

**Table 167: Address Resolution Protocol Commands**

Command	Function	Mode
<a href="#">arp</a>	Adds a static entry in the ARP cache	GC
<a href="#">ip proxy-arp</a>	Enables proxy ARP service	IC
<a href="#">clear arp-cache</a>	Deletes all dynamic entries from the ARP cache	PE
<a href="#">show arp</a>	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 128.
- ◆ 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 \(791\)](#)  
[show arp \(791\)](#)

**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

### 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. The first line shows the cache timeout. 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.

### Example

This example displays all entries in the ARP cache.

```

Console#show arp
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address      Type      Interface
-----
10.1.0.0        FF-FF-FF-FF-FF other      VLAN1
10.1.0.254     00-00-AB-CD-00 other      VLAN1
10.1.0.255     FF-FF-FF-FF-FF other      VLAN1
145.30.20.23   09-50-40-30-20 dynamic  VLAN3

Total entry : 4
Console#

```

## IPv6 Interface

This switch supports the following IPv6 interface commands.

**Table 168: 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



Table 168: IPv6 Configuration Commands (Continued)

Command	Function	Mode
<code>traceroute6</code>	Shows the route packets take to the specified host	PE
<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 \(802\)](#)

[ip default-gateway \(784\)](#)

**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 \(797\)](#)  
[ipv6 address autoconfig \(795\)](#)  
[show ipv6 interface \(802\)](#)  
[ip address \(782\)](#)

**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 \(794\)](#)

[show ipv6 interface \(802\)](#)

**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 \(795\)](#)

[show ipv6 interface \(802\)](#)

**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 \(800\)](#)

[show ipv6 interface \(802\)](#)

**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 797](#)). 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 \(799\)](#)

[show ipv6 interface \(802\)](#)

**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

- ◆ If a non-default value is configured, an MTU option is included in the router advertisements sent from this device.
- ◆ 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 \(805\)](#)

[jumbo frame \(102\)](#)

**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: 1-4094)

*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 169: 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

**Table 169: show ipv6 interface - display description** (Continued)

Field	Description
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.
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:CFF:FE00:FD%1/64
Console#

```

**Related Commands**

[show ip interface \(785\)](#)

**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 170: 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 171: 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.

**Table 171: show ipv6 traffic - display description** (Continued)

Field	Description
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.
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.
reassemble 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.
reassemble 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.
reassemble 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> .

**Table 171: show ipv6 traffic - display description** (Continued)

Field	Description
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.
<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>ipv6IfcmlnErrors</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.



**Table 171: show ipv6 traffic - display description** (Continued)

Field	Description
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 icmpOutErrors.
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.
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::2727%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 761](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 762](#)).
- ◆ 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:CFE:FE9C:CA10%1
Press "ESC" to abort.

Traceroute to FE80::2E0:CFE: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:CFE:FE9C:CA10%1/64

Trace completed.
Console#
```

## Neighbor Discovery

**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:CFE:FE9C:CA10                    4    00-E0-0C-9C-CA-10 R      1
Console#

```

**Table 172: 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	The following states are used for dynamic entries: 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. I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293). 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. 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.

**Table 172: 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: I1 (Incomplete)-The interface for this entry is down. R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache. P2 (Permanent) - Indicates a static entry.</p>
VLAN	VLAN interface from which the address was reached.

### Related Commands

[show mac-address-table \(438\)](#)

---

# 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
<a href="#">Global Routing Configuration</a>	Configures global parameters for static routing, displays the routing table

---

## Global Routing Configuration

**Table 161: Global Routing Configuration Commands**

Command	Function	Mode
<i>IPv4 Commands</i>		
<a href="#">ip route</a>	Configures static routes	GC
<a href="#">show ip route</a>	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. (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 56 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** | **static** | **summary**]

**connected** – Displays all currently connected entries.

**database** – All known routes, including inactive routes.

**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       127.0.0.0/8 is directly connected, lo
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    *> 127.0.0.0/8 is directly connected, lo0
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#
```

# Section III

## Appendices

This section provides additional information and includes these items:

- ◆ [“Troubleshooting” on page 821](#)
- ◆ [“License Information” on page 823](#)





# Troubleshooting

## Problems Accessing the Management Interface

Table 162: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, or SNMP software	<ul style="list-style-type: none"><li>◆ Be sure the switch is powered up.</li><li>◆ 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.</li><li>◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled.</li><li>◆ 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.</li><li>◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.</li><li>◆ 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.</li><li>◆ 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.</li></ul>
Cannot connect using Secure Shell	<ul style="list-style-type: none"><li>◆ 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.</li><li>◆ 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.</li><li>◆ 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.</li><li>◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.</li><li>◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).</li></ul>
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none"><li>◆ 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.</li><li>◆ 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.</li></ul>
Forgot or lost the password	<ul style="list-style-type: none"><li>◆ Contact your local distributor.</li></ul>

## 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.

**BGP** Border Gateway Protocol is a protocol used to make core routing decisions on the Internet. It maintains a table of IP networks to register reachability among autonomous systems (AS). BGP makes routing decisions based on path, network policies and/or rule-sets.

**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.
- GVRP** GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

- 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.

**MVR** Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard groups.

**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.

**OSPF** Open Shortest Path First is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

**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.
- VRRP** Virtual Router Redundancy Protocol uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

**XModem** A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

---

# List of Commands

## A

aaa accounting commands 217  
aaa accounting dot1x 218  
aaa accounting exec 219  
aaa accounting update 220  
aaa authorization commands 220  
aaa authorization exec 221  
aaa group server 222  
absolute 152  
access-list arp 366  
access-list ip 348  
access-list ipv6 354  
access-list mac 361  
accounting commands 224  
accounting dot1x 223  
accounting exec 224  
arp 789  
authentication enable 206  
authentication login 207  
authorization commands 225  
authorization exec 226

## B

boot system 104  
bridge-ext gvrp 474

## C

calendar set 150  
capabilities 373  
channel-group 404  
class 570  
class-map 566  
clear access-list hardware counters 369  
clear arp-cache 791  
clear collision-mac-address-table 437  
clear counters 380  
clear dns cache 765  
clear efm oam counters 752  
clear efm oam event-log 752  
clear erps statistics 543  
clear ethernet cfm ais mpid 717  
clear ethernet cfm errors 729  
clear ethernet cfm linktrace-cache 738  
clear ethernet cfm maintenance-points remote 728  
clear host 765  
clear ip dhcp snooping binding 303  
clear ip dhcp snooping database flash 303  
clear ip igmp snooping groups dynamic 595

clear ip igmp snooping statistics 595  
clear ip source-guard binding blocked 320  
clear ipv6 dhcp snooping binding 312  
clear ipv6 dhcp snooping statistics 313  
clear ipv6 mld snooping groups dynamic 623  
clear ipv6 mld snooping statistics 624  
clear ipv6 neighbors 812  
clear ipv6 traffic 810  
clear log 131  
clear mac-address-table dynamic 437  
clear mvr groups dynamic 652  
clear mvr statistics 652  
clear mvr6 groups dynamic 673  
clear mvr6 statistics 674  
clear network-access 282  
clear pppoe intermediate-agent statistics 264  
clock summer-time (date) 145  
clock summer-time (predefined) 147  
clock summer-time (recurring) 148  
clock timezone 149  
cluster 155  
cluster commander 156  
cluster ip-pool 157  
cluster member 158  
configure 85  
control-vlan 524  
copy 105

## D

databits 118  
delete 109  
delete public-key 240  
description 567  
description 374  
dir 110  
disable 86  
discard 375  
disconnect 125  
dos-protection echo-charge 337  
dos-protection smurf 337  
dos-protection tcp-flooding 338  
dos-protection tcp-null-scan 338  
dos-protection tcp-syn-fin-scan 339  
dos-protection tcp-xmas-scan 339  
dos-protection udp-flooding 340  
dos-protection win-nuke 340  
dot1q-tunnel system-tunnel-control 489  
dot1x default 246  
dot1x intrusion-action 247

## List of Commands

dot1x max-reauth-req 248  
dot1x max-req 248  
dot1x operation-mode 249  
dot1x port-control 250  
dot1x re-authenticate 253  
dot1x re-authentication 250  
dot1x system-auth-control 246  
dot1x timeout auth-period 254  
dot1x timeout held-period 254  
dot1x timeout quiet-period 251  
dot1x timeout re-authperiod 251  
dot1x timeout supp-timeout 252  
dot1x timeout tx-period 252

## E

efm oam 748  
efm oam critical-link-event 748  
efm oam link-monitor frame threshold 750  
efm oam link-monitor frame window 750  
efm oam link-monitor frame 749  
efm oam mode 751  
efm oam remote-loopback 753  
efm oam remote-loopback test 754  
enable 525  
enable 83  
enable password 202  
end 87  
erps 523  
erps clear 543  
erps domain 524  
erps forced-switch 544  
erps manual-switch 546  
ethernet cfm ais level 708  
ethernet cfm ais ma 709  
ethernet cfm ais period 710  
ethernet cfm ais suppress alarm 710  
ethernet cfm cc enable 726  
ethernet cfm cc ma interval 725  
ethernet cfm delay-measure two-way 744  
ethernet cfm domain 711  
ethernet cfm enable 713  
ethernet cfm linktrace 736  
ethernet cfm linktrace cache 734  
ethernet cfm linktrace cache hold-time 735  
ethernet cfm linktrace cache size 736  
ethernet cfm loopback 739  
ethernet cfm mep 716  
ethernet cfm mep crosscheck 733  
ethernet cfm mep crosscheck start-delay 731  
ethernet cfm port-enable 717  
exec-timeout 118  
exit 87

## F

flowcontrol 375

## G

garp timer 475  
guard-timer 526

## H

history 376  
holdoff-timer 527  
hostname 90

## I

interface 372  
interface vlan 482  
ip access-group 352  
ip address 782  
ip arp inspection 328  
ip arp inspection filter 329  
ip arp inspection limit 333  
ip arp inspection log-buffer logs 330  
ip arp inspection trust 333  
ip arp inspection validate 331  
ip arp inspection vlan 332  
ip default-gateway 784  
ip dhcp client class-id 771  
ip dhcp dynamic-provision 770  
ip dhcp relay server 777  
ip dhcp restart client 773  
ip dhcp restart relay 778  
ip dhcp snooping 291  
ip dhcp snooping max-number 301  
ip dhcp snooping database flash 303  
ip dhcp snooping information option 293  
ip dhcp snooping information option circuit-id 300  
ip dhcp snooping information option encode no-subtype 294  
ip dhcp snooping information option remote-id 296  
ip dhcp snooping information option tr101 board-id 297  
ip dhcp snooping information policy 297  
ip dhcp snooping trust 302  
ip dhcp snooping verify mac-address 298  
ip dhcp snooping vlan 299  
ip domain-list 760  
ip domain-lookup 761  
ip domain-name 762  
ip host 762  
ip http authentication 229  
ip http port 229  
ip http secure-port 230  
ip http secure-server 231  
ip http server 230  
ip igmp authentication 605  
ip igmp filter (Global Configuration) 603  
ip igmp filter (Interface Configuration) 607  
ip igmp max-groups 608  
ip igmp max-groups action 608  
ip igmp profile 604  
ip igmp query-drop 609

ip igmp snooping 579  
 ip igmp snooping priority 580  
 ip igmp snooping proxy-reporting 580  
 ip igmp snooping querier 581  
 ip igmp snooping router-alert-option-check 582  
 ip igmp snooping router-port-expire-time 582  
 ip igmp snooping tcn-flood 583  
 ip igmp snooping tcn-query-solicit 584  
 ip igmp snooping unregistered-data-flood 585  
 ip igmp snooping unsolicited-report-interval 585  
 ip igmp snooping version 586  
 ip igmp snooping version-exclusive 587  
 ip igmp snooping vlan general-query-suppression 587  
 ip igmp snooping vlan immediate-leave 588  
 ip igmp snooping vlan last-memb-query-count 589  
 ip igmp snooping vlan last-memb-query-intvl 590  
 ip igmp snooping vlan mrd 590  
 ip igmp snooping vlan mrouter 601  
 ip igmp snooping vlan proxy-address 591  
 ip igmp snooping vlan query-interval 593  
 ip igmp snooping vlan query-resp-intvl 593  
 ip igmp snooping vlan static 594  
 ip mdns 767  
 ip multicast-data-drop 609  
 ip name-server 763  
 ip proxy-arp 790  
 ip route 816  
 ip source-guard 317  
 ip source-guard binding 315  
 ip source-guard max-binding 318  
 ip source-guard mode 319  
 ip ssh authentication-retries 238  
 ip ssh crypto host-key generate 241  
 ip ssh crypto zeroize 242  
 ip ssh save host-key 242  
 ip ssh server 238  
 ip ssh server-key size 239  
 ip ssh timeout 240  
 ip telnet max-sessions 233  
 ip telnet port 233  
 ip telnet server 234  
 ip tftp retry 114  
 ip tftp timeout 115  
 ipv6 access-group 359  
 ipv6 address 794  
 ipv6 address autoconfig 795  
 ipv6 address eui-64 797  
 ipv6 address link-local 799  
 ipv6 default-gateway 793  
 ipv6 dhcp client rapid-commit vlan 774  
 ipv6 dhcp restart client vlan 774  
 ipv6 dhcp snooping 305  
 ipv6 dhcp snooping max-binding 311  
 ipv6 dhcp snooping option remote-id 308  
 ipv6 dhcp snooping option remote-id policy 309  
 ipv6 dhcp snooping trust 311  
 ipv6 dhcp snooping vlan 310  
 ipv6 enable 800  
 ipv6 host 764  
 ipv6 mld filter (Global Configuration) 631  
 ipv6 mld filter (Interface Configuration) 634  
 ipv6 mld max-groups 635  
 ipv6 mld max-groups action 635  
 ipv6 mld profile 632  
 ipv6 mld query-drop 636  
 ipv6 mld snooping 615  
 ipv6 mld snooping proxy-reporting 615  
 ipv6 mld snooping querier 616  
 ipv6 mld snooping query-interval 617  
 ipv6 mld snooping query-max-response-time 617  
 ipv6 mld snooping robustness 618  
 ipv6 mld snooping router-port-expire-time 618  
 ipv6 mld snooping unknown-multicast mode 619  
 ipv6 mld snooping unsolicited-report-interval 620  
 ipv6 mld snooping version 620  
 ipv6 mld snooping vlan immediate-leave 621  
 ipv6 mld snooping vlan mrouter 622  
 ipv6 mld snooping vlan static 623  
 ipv6 mtu 801  
 ipv6 multicast-data-drop 636  
 ipv6 source-guard 324  
 ipv6 source-guard binding 322  
 ipv6 source-guard max-binding 325

## J

jumbo frame 102

## L

l2protocol-tunnel tunnel-dmac 498  
 lacp 405  
 lacp admin-key (Ethernet Interface) 406  
 lacp admin-key (Port Channel) 409  
 lacp port-priority 407  
 lacp system-priority 408  
 lacp timeout 410  
 line 117  
 lldp 683  
 lldp admin-status 687  
 lldp basic-tlv management-ip-address 687  
 lldp basic-tlv port-description 688  
 lldp basic-tlv system-capabilities 688  
 lldp basic-tlv system-description 689  
 lldp basic-tlv system-name 689  
 lldp dot1-tlv proto-ident 690  
 lldp dot1-tlv proto-vid 690  
 lldp dot1-tlv pvid 691  
 lldp dot1-tlv vlan-name 691  
 lldp dot3-tlv link-agg 692  
 lldp dot3-tlv mac-phy 692  
 lldp dot3-tlv max-frame 693  
 lldp holdtime-multiplier 683  
 lldp med-fast-start-count 684  
 lldp med-location civic-addr 694  
 lldp med-notification 695  
 lldp med-tlv inventory 696

## List of Commands

lldp med-tlv location 697  
lldp med-tlv med-cap 697  
lldp med-tlv network-policy 698  
lldp notification 698  
lldp notification-interval 684  
lldp refresh-interval 685  
lldp reinit-delay 685  
lldp tx-delay 686  
logging command 127  
logging facility 128  
logging history 128  
logging host 129  
logging on 130  
logging sendmail 135  
logging sendmail destination-email 135  
logging sendmail host 136  
logging sendmail level 136  
logging sendmail source-email 137  
logging trap 131  
login 119  
loopback detection trap 432  
loopback-detection 430  
loopback-detection action 430  
loopback-detection recover-time 431  
loopback-detection release 433  
loopback-detection transmit-interval 432

## M

ma index name 714  
ma index name-format 715  
mac access-group 364  
mac-address-table aging-time 435  
mac-address-table static 436  
mac-authentication intrusion-action 281  
mac-authentication max-mac-count 281  
mac-authentication reauth-time 275  
mac-learning 268  
mac-vlan 511  
major-domain 527  
management 257  
match 568  
max-hops 451  
media-type 377  
meg-level 528  
memory 182  
mep archive-hold-time 728  
mep crosscheck mpid 732  
mep fault-notify alarm-time 740  
mep fault-notify lowest-priority 741  
mep fault-notify reset-time 742  
mep-monitor 529  
mst priority 451  
mst vlan 452  
mvr 641  
mvr associated-profile 641  
mvr domain 642  
mvr immediate-leave 649  
mvr priority 643

mvr profile 643  
mvr proxy-query-interval 644  
mvr proxy-switching 645  
mvr robustness-value 646  
mvr source-port-mode dynamic 647  
mvr type 650  
mvr upstream-source-ip 647  
mvr vlan 648  
mvr vlan group 651  
mvr6 associated-profile 663  
mvr6 domain 663  
mvr6 immediate-leave 670  
mvr6 priority 664  
mvr6 profile 665  
mvr6 proxy-query-interval 666  
mvr6 proxy-switching 666  
mvr6 robustness-value 667  
mvr6 source-port-mode dynamic 668  
mvr6 type 671  
mvr6 upstream-source-ip 669  
mvr6 vlan 669  
mvr6 vlan group 672

## N

name 453  
negotiation 377  
network-access aging 273  
network-access dynamic-qos 276  
network-access dynamic-vlan 277  
network-access guest-vlan 278  
network-access mac-filter 274  
network-access max-mac-count 278  
network-access mode mac-authentication 279  
network-access port-mac-filter 280  
nlm 179  
no rspan session 423  
node-id 530  
non-erps-dev-protect 530  
non-revertive 532  
ntp authenticate 142  
ntp authentication-key 142  
ntp client 143  
ntp server 144

## P

parity 120  
password 121  
password-thresh 121  
periodic 153  
permit, deny 604  
permit, deny 633  
permit, deny (ARP ACL) 367  
permit, deny (Extended IPv4 ACL) 349  
permit, deny (Extended IPv6 ACL) 356  
permit, deny (MAC ACL) 361  
permit, deny (Standard IP ACL) 348  
permit, deny (Standard IPv6 ACL) 355

ping 788  
ping6 810  
police rate 571  
policy-map 570  
port channel load-balance 402  
port monitor 415  
port security 269  
power-save 399  
pppoe intermediate-agent 260  
pppoe intermediate-agent format-type 260  
pppoe intermediate-agent port-enable 261  
pppoe intermediate-agent port-format-type 262  
pppoe intermediate-agent trust 263  
pppoe intermediate-agent vendor-tag strip 264  
privilege 205  
process cpu 183  
process cpu guard 184  
prompt 81  
propagate-tc 535  
protocol-vlan protocol-group (Configuring Groups) 505  
protocol-vlan protocol-group (Configuring Interfaces) 506

## Q

qos map cos-queue 558  
qos map dscp-queue 560  
qos map trust-mode 561  
queue mode 554  
queue weight 555  
quit 84

## R

radius-server auth-port 209  
radius-server host 209  
radius-server key 210  
radius-server retransmit 211  
radius-server timeout 211  
range 605  
range 633  
raps-def-mac 536  
raps-without-vc 537  
rate-limit 426  
rcommand 158  
reload (Global Configuration) 82  
reload (Privileged Exec) 86  
rename 569  
revision 453  
ring-port 539  
rmon alarm 188  
rmon collection history 190  
rmon collection rmon1 191  
rmon event 189  
rpl neighbor 540  
rpl owner 540  
rspan destination 421  
rspan remote vlan 422

rspan source 420

## S

radius-server acct-port 208  
server 223  
service-policy 574  
set cos 572  
set ip dscp 573  
sflow owner 195  
sflow polling instance 197  
sflow sampling instance 198  
show access-group 369  
show access-list 370  
show access-list arp 368  
show access-list tcam-utilization 91  
show accounting 226  
show arp 791  
show authorization 227  
show bridge-ext 477  
show cable-diagnostics 398  
show calendar 151  
show class-map 574  
show cluster 159  
show cluster candidates 160  
show cluster members 159  
show collision-mac-address-table 437  
show dns 766  
show dns cache 766  
show dos-protection 341  
show dot1q-tunnel 497  
show dot1q-tunnel service 496  
show dot1x 255  
show efm oam counters interface 755  
show efm oam event-log interface 755  
show efm oam remote-loopback interface 757  
show efm oam status remote interface 758  
show efm oam status interface 757  
show erps 547  
show ethernet cfm configuration 718  
show ethernet cfm errors 730  
show ethernet cfm fault-notify-generator 743  
show ethernet cfm linktrace-cache 738  
show ethernet cfm ma 720  
show ethernet cfm maintenance-points local 721  
show ethernet cfm maintenance-points local detail mep 722  
show ethernet cfm maintenance-points remote crosscheck 734  
show ethernet cfm maintenance-points remote detail 723  
show ethernet cfm md 720  
show garp timer 478  
show gvrp configuration 479  
show history 84  
show hosts 767  
show interfaces brief 381  
show interfaces counters 381  
show interfaces history 385



## List of Commands

show interfaces protocol-vlan protocol-group 508  
show interfaces status 387  
show interfaces switchport 388  
show interfaces transceiver 395  
show interfaces transceiver-threshold 396  
show ip access-group 353  
show ip access-list 353  
show ip arp inspection configuration 334  
show ip arp inspection interface 334  
show ip arp inspection log 335  
show ip arp inspection statistics 335  
show ip arp inspection vlan 335  
show ip default-gateway 785  
show ip dhcp dynamic-provision 773  
show ip dhcp snooping 304  
show ip dhcp snooping binding 304  
show ip igmp authentication 610  
show ip igmp filter 611  
show ip igmp profile 611  
show ip igmp query-drop 612  
show ip igmp snooping 596  
show ip igmp snooping group 597  
show ip igmp snooping mrouter 598  
show ip igmp snooping statistics 598  
show ip igmp throttle interface 612  
show ip interface 785  
show ip mdns 768  
show ip multicast-data-drop 613  
show ip route 817  
show ip source-guard 320  
show ip source-guard binding 321  
show ip ssh 243  
show ip telnet 235  
show ip tftp 115  
show ip traffic 786  
show ipv6 access-group 359  
show ipv6 access-list 360  
show ipv6 default-gateway 802  
show ipv6 dhcp duid 776  
show ipv6 dhcp snooping 313  
show ipv6 dhcp snooping binding 313  
show ipv6 dhcp snooping statistics 314  
show ipv6 dhcp vlan 776  
show ipv6 interface 802  
show ipv6 mld filter 637  
show ipv6 mld profile 638  
show ipv6 mld query-drop 638  
show ipv6 mld snooping group 625  
show ipv6 mld snooping group source-list 625  
show ipv6 mld snooping mrouter 626  
show ipv6 mld snooping statistics 627  
show ipv6 mld throttle interface 639  
show ipv6 mld snooping 624  
show ipv6 mtu 805  
show ipv6 neighbors 813  
show ipv6 source-guard 326  
show ipv6 source-guard binding 327  
show ipv6 traffic 805  
show l2protocol-tunnel 502  
show lacp 411  
show line 126  
show lldp config 699  
show lldp info local-device 700  
show lldp info remote-device 701  
show lldp info statistics 703  
show log 132  
show logging 133  
show logging sendmail 138  
show loopback-detection 434  
show mac access-group 365  
show mac access-list 365  
show mac-address-table 438  
show mac-address-table aging-time 439  
show mac-address-table count 439  
show mac-vlan 512  
show management 258  
show memory 92  
show mvr 653  
show mvr associated-profile 654  
show mvr interface 654  
show mvr members 655  
show mvr profile 657  
show mvr statistics 658  
show mvr6 674  
show mvr6 associated-profile 675  
show mvr6 interface 676  
show mvr6 members 677  
show mvr6 profile 678  
show mvr6 statistics 679  
show network-access 282  
show network-access mac-address-table 283  
show network-access mac-filter 284  
show nlm oper-status 182  
show ntp 145  
show policy-map 575  
show policy-map interface 576  
show port monitor 417  
show port security 271  
show port-channel load-balance 414  
show power-save 400  
show pppoe intermediate-agent info 265  
show pppoe intermediate-agent statistics 265  
show privilege 205  
show process cpu 93  
show process cpu guard 93  
show process cpu task 94  
show protocol-vlan protocol-group 507  
show public-key 243  
show qos map cos-queue 562  
show qos map dscp-queue 563  
show qos map trust-mode 563  
show queue mode 557  
show queue weight 557  
show radius-server 212  
show reload 87  
show rmon alarms 192  
show rmon events 192  
show rmon history 193



show rmon statistics 193  
 show rspan 424  
 show running-config 96  
 show sflow 199  
 show snmp 165  
 show snmp engine-id 176  
 show snmp group 177  
 show snmp notify-filter 182  
 show snmp user 178  
 show snmp view 179  
 show snmp-server enable port-traps 170  
 show snmp 141  
 show spanning-tree 468  
 show spanning-tree mst configuration 470  
 show spanning-tree tc-prop 471  
 show ssh 244  
 show startup-config 97  
 show subnet-vlan 510  
 show system 98  
 show tacacs-server 215  
 show tech-support 99  
 show time-range 154  
 show traffic-segmentation 345  
 show upgrade 114  
 show users 100  
 show version 101  
 show vlan 487  
 show vlan-translation 504  
 show voice vlan 518  
 show watchdog 101  
 show web-auth 289  
 show web-auth interface 289  
 show web-auth summary 290  
 shutdown 378  
 silent-time 122  
 snmp-server 163  
 snmp-server community 163  
 snmp-server contact 164  
 snmp-server enable traps ethernet cfm cc 727  
 snmp-server enable traps ethernet cfm crosscheck 731  
 snmp-server enable port-traps link-up-down 169  
 snmp-server enable port-traps mac-notification 170  
 snmp-server enable traps 166  
 snmp-server engine-id 171  
 snmp-server group 172  
 snmp-server host 167  
 snmp-server location 165  
 snmp-server notify-filter 180  
 snmp-server user 173  
 snmp-server view 175  
 snmp client 139  
 snmp poll 140  
 snmp server 140  
 spanning-tree 442  
 spanning-tree bpdu-filter 454  
 spanning-tree bpdu-guard 455  
 spanning-tree cisco-prestandard 443  
 spanning-tree cost 456  
 spanning-tree edge-port 457  
 spanning-tree forward-time 444  
 spanning-tree hello-time 444  
 spanning-tree link-type 458  
 spanning-tree loopback-detection 458  
 spanning-tree loopback-detection action 459  
 spanning-tree loopback-detection release 467  
 spanning-tree loopback-detection release-mode 460  
 spanning-tree loopback-detection trap 461  
 spanning-tree max-age 445  
 spanning-tree mode 446  
 spanning-tree mst configuration 447  
 spanning-tree mst cost 462  
 spanning-tree mst port-priority 463  
 spanning-tree pathcost method 447  
 spanning-tree port-bpdu-flooding 463  
 spanning-tree port-priority 464  
 spanning-tree priority 448  
 spanning-tree protocol-migration 467  
 spanning-tree restricted-tcn 461  
 spanning-tree root-guard 465  
 spanning-tree spanning-disabled 466  
 spanning-tree system-bpdu-flooding 449  
 spanning-tree tc-prop 449  
 spanning-tree tc-prop-stop 466  
 spanning-tree transmission-limit 450  
 speed 123  
 speed-duplex 379  
 stopbits 123  
 subnet-vlan 509  
 switchport acceptable-frame-types 483  
 switchport allowed vlan 483  
 switchport dot1q-tunnel mode 490  
 switchport dot1q-tunnel priority map 491  
 switchport dot1q-tunnel service default match all discard 491  
 switchport dot1q-tunnel service default match untagged discard 492  
 switchport dot1q-tunnel service match cvid 492  
 switchport dot1q-tunnel tpid 495  
 switchport forbidden vlan 476  
 switchport gvrp 476  
 switchport ingress-filtering 485  
 switchport l2protocol-tunnel 501  
 switchport mode 485  
 switchport native vlan 486  
 switchport packet-rate 427  
 switchport priority default 556  
 switchport vlan-translation 502  
 switchport voice vlan 516  
 switchport voice vlan priority 516  
 switchport voice vlan rule 517  
 switchport voice vlan security 518

**T**

tacacs-server host 213  
 tacacs-server key 213  
 tacacs-server port 214

---

## List of Commands

tacacs-server retransmit 214  
tacacs-server timeout 215  
telnet (client) 234  
terminal 125  
test cable-diagnostics 397  
timeout login response 124  
time-range 151  
traceroute 787  
traceroute6 811  
traffic-segmentation 342  
traffic-segmentation session 343  
traffic-segmentation uplink/downlink 343  
traffic-segmentation uplink-to-uplink 344  
transceiver-monitor 389  
transceiver-threshold current 390  
transceiver-threshold rx-power 391  
transceiver-threshold temperature 392  
transceiver-threshold tx-power 393  
transceiver-threshold voltage 394  
transceiver-threshold-auto 390

## U

upgrade opcode auto 111  
upgrade opcode path 113  
upgrade opcode reload 114  
username 203

## V

version 541  
vlan 480  
vlan database 479  
voice vlan 513  
voice vlan aging 514  
voice vlan mac-address 515

## W

watchdog software 102  
web-auth 287  
web-auth login-attempts 285  
web-auth quiet-period 286  
web-auth re-authenticate (IP) 288  
web-auth re-authenticate (Port) 288  
web-auth session-timeout 286  
web-auth system-auth-control 287  
whichboot 111  
wtr-timer 542

---

# Index

## Numerics

- 802.1Q tunnel 488
  - access 490
  - CVID to SVID map 492
  - ethernet type 495
  - interface configuration 490–495
  - mode selection 490
  - status, configuring 489
  - TPID 495
  - uplink 490
- 802.1X
  - authenticator, configuring 247–253
  - global settings 246
  - port authentication 245, 246
  - port authentication accounting 223

## A

- AAA
  - accounting 802.1X port settings 223
  - accounting exec command privileges 219, 224, 225
  - accounting exec settings 224
  - accounting summary 226
  - accounting update 220
  - accounting, configuring 216
  - authorization & accounting 216
  - authorization exec settings 221
  - authorization method 221
  - authorization settings 221
  - authorization summary 226
  - RADIUS group settings 222
  - TACACS+ group settings 222
- acceptable frame type 483
- Access Control List *See* ACL
- ACL 347
  - ARP 366
  - IPv4 Extended 347, 349
  - IPv4 Standard 347, 348
  - IPv6 Extended 354, 356
  - IPv6 Standard 354, 355
  - MAC 360
  - time range 151
- address table 435
  - aging time 435
  - aging time, displaying 439
  - aging time, setting 435

- administrative users, displaying 100
- ARP
  - proxy 790
- ARP ACL 329
- ARP configuration 789
- ARP inspection 327
  - ACL filter 329
  - additional validation criteria 331
  - ARP ACL 366
  - enabling globally 328
  - enabling per VLAN 332
  - trusted ports 333
- ARP statistics 786
- ATC 145
- authentication
  - MAC address authentication 273, 279
  - MAC, configuring ports 273
  - network access 273, 279
  - public key 237
  - web 287
  - web authentication port information, displaying 289
  - web authentication, configuring ports 287
  - web authentication, re-authenticating address 288
  - web authentication, re-authenticating ports 288
  - web, configuring 287

## B

- BOOTP 782
- BPDU
  - filter 454
  - flooding when STA disabled on VLAN 463
  - flooding when STA globally disabled 449
  - ignoring superior BPDUs 465
  - selecting protocol based on message format 467
  - shut down port on receipt 455
- bridge extension capabilities, displaying 477
- broadcast storm, threshold 427

## C

- cable diagnostics 397
- CDP, discard 375
- CFM
  - continuity check errors 729, 730
  - continuity check messages 531, 705, 725, 726
  - cross-check errors 727, 731, 733

## Index

- cross-check message 705, 731, 733, 734
  - cross-check start delay 731
  - delay measure 744
  - domain service access point 712
  - fault isolation 705, 737
  - fault notification 705, 740, 741, 742
  - fault notification generator 741, 743
  - fault verification 705
  - link trace cache 735, 736, 738
  - link trace message 705, 734, 735, 736
  - loop back messages 705, 739
  - maintenance association 705, 714, 720
  - maintenance domain 705, 711, 720
  - maintenance end point 712, 716, 721
  - maintenance intermediate point 711, 712, 714, 721
  - maintenance level 711
  - maintenance point 705, 721
  - MEP archive 728
  - MEP direction 716
  - remote maintenance end point 722, 723, 728, 732
  - service instance 714
  - SNMP traps 727, 731
  - class map
    - description 567
    - DiffServ 566
  - CLI
    - command modes 74
    - showing commands 72
  - clustering switches, management access 155
  - command line interface *See* CLI
  - committed information rate, QoS policy 571
  - community string 53, 163
  - configuration file, DHCP download reference 62
  - configuration files, restoring defaults 103
  - configuration settings
    - restoring 56, 103, 105
    - saving 56, 103, 105
  - configuration settings, automatic installation 62
  - console port, required connections 44
  - continuity check errors, CFM 729, 730
  - continuity check messages, CFM 531, 705, 725, 726
  - CoS 561
    - configuring 553
    - enabling 561
    - layer 3/4 priorities 558
    - queue mode 554
    - queue weights, assigning 555
  - CPU
    - status 93
    - tasks, showing 94
    - utilization, setting trap 183
    - utilization, showing 93
  - cross-check errors, CFM 727, 731, 733
  - cross-check message, CFM 705, 731, 733, 734
  - cross-check start delay, CFM 731
  - CVLAN to SPVLAN map 492
- ## D
- Daylight Savings Time *See* summer time
  - default IPv4 gateway, configuration 784
  - default IPv6 gateway, configuration 793
  - default priority, ingress port 556
  - delay measure, CFM 744
  - DHCP 782
    - class identifier 771
    - client 769, 782
    - client identifier 771
    - dynamic configuration 51
    - relay 777
    - relay service, enabling 778
  - DHCP snooping
    - information option, circuit ID 300
    - subtype field 294
  - DHCPv4 snooping 290
    - enabling 291
    - global configuration 291
    - information option 293, 296
    - information option policy 297
    - information option, enabling 293, 296
    - information option, remote ID 293
    - policy selection 297
    - remote ID 296
    - specifying trusted interfaces 302
    - sub-length field 294
    - sub-option format 294
    - sub-type and sub-length, disabling 294
    - subtype field 294
    - verifying MAC addresses 298
    - VLAN configuration 299
  - DHCPv6 snooping 305
    - enabling 305
    - global configuration 305
    - remote id policy, option 37 309
    - remote ID, option 37 308
    - specifying trusted interfaces 311
    - trusted port 311
    - untrusted port 311
    - VLAN configuration 310
  - DiffServ 565
    - binding policy to interface 574
    - class map 566, 570
    - class map, description 567
    - classifying QoS traffic 568
    - committed information rate 571
    - configuring 565
    - description 567
    - policy map 570
    - policy map, description 567

- QoS policy 570
- service policy 574
- setting CoS for matching packets 572
- setting IP DSCP for matching packets 573

**DNS**

- default domain name 762
- displaying the cache 766
- domain name list 762, 764
- enabling lookup 761
- name server list 763
- static entries, IPv4 762
- static entries, IPv6 764

Domain Name Service *See* DNS

domain service access point, CFM 712

DoS protection 336

downloading software 105

- automatically 111
- using TFTP 105

DSA encryption 241

DSCP 561

- enabling 561

dynamic addresses

- clearing 437
- displaying 438

Dynamic Host Configuration Protocol *See* DHCP

dynamic QoS assignment 276

dynamic VLAN assignment 277

**E**

- edge port, STA 457
- encryption
  - DSA 241
  - RSA 241
- engine ID 171

**ERPS**

- configuration guidelines 522
- control VLAN 524
- domain configuration 524
- domain, enabling 525
- global configuration 523
- guard timer 526
- hold-off timer 527
- major domain 527
- MEG level 528
- node identifier 530
- non-compliant device protection 530
- non-ERPS device protection 530
- propagate topology change 535
- ring configuration 524
- ring port, east interface 539
- ring port, west interface 539
- ring, enabling 525
- RPL owner 540
- secondary ring 527

- status, displaying 547
- wait-to-restore expire timer 550
- wait-to-restore timer 542
- WTR expire 550
- WTR timer 542

Ethernet Ring Protection Switching *See* ERPS

- event logging 127
- exec command privileges, accounting 219, 224, 225
- exec settings
  - accounting 224
  - authorization 221

**F**

- fault isolation, CFM 705, 737
- fault notification generator, CFM 741, 743
- fault notification, CFM 705, 740, 741, 742
- fault verification, CFM 705
- FIB, description 817
- firmware
  - displaying version 101
  - upgrading 105
  - upgrading automatically 111
  - upgrading with FTP or TFP 111
  - version, displaying 101
- forwarding information base *See* FIB

**G**

- gateway, IPv4 default 784
- gateway, IPv6 default 793
- general security measures 267
- GNU license 823
- GVRP
  - enabling 474
  - global setting 474
  - interface configuration 476

**H**

- hardware version, displaying 101
- HTTP, web server 230
- HTTPS 231
  - configuring 230, 231
  - replacing SSL certificate 105, 109
  - secure-site certificate 105, 109
- HTTPS, secure server 231

**I**

- IEEE 802.1D 446
- IEEE 802.1s 446
- IEEE 802.1w 446
- IEEE 802.1X 245, 246

## Index

### IGMP

- filter profiles, binding to interface 607
- filter profiles, configuration 604
- filter, interface configuration 605–608
- filter, parameters 603–608
- filtering & throttling 602
- filtering & throttling, enabling 603
- filtering & throttling, interface configuration 605–609
- filtering & throttling, status 603
- filtering, configuring profile 604, 605
- filtering, creating profile 604
- filtering, group range 605
- filtering, interface settings 607–608
- groups, displaying 597
- Layer 2 577
- query 581
- query, enabling 581
- RADIUS authentication 605
- snooping 577
- snooping & query, parameters 577
- snooping, configuring 577
- snooping, enabling 579
- snooping, immediate leave 588

IGMP snooping

- configuring 577
- enabling per interface 579
- forwarding entries 597
- immediate leave, status 588
- interface attached to multicast router 598, 601
- last member query count 589
- last member query interval 590
- proxy query address 591
- proxy query interval 593
- proxy query response interval 593
- proxy reporting 580, 615
- querier timeout 582
- querier, enabling 581
- router port expire time 582
- static host interface 594
- static multicast routing 601
- static port assignment 594
- static router interface 601
- static router port, configuring 601
- statistics, displaying 598, 627
- TCN flood 583
- unregistered data flooding 585
- version exclusive 587
- version for interface, setting 586
- version, setting 586
- with proxy reporting 580, 615

immediate leave, IGMP snooping 588

immediate leave, MLD snooping 621

importing user public keys 105, 109

ingress filtering 485

IP address, setting 781

IP filter, for management access 257

IP routing 815

- unicast protocols 815

IP source guard

- configuring static entries 315
- setting filter criteria 317
- setting maximum bindings 318, 319

IP statistics 786

IPv4 address

- BOOTP/DHCP 773, 782
- dynamic configuration 51
- manual configuration 48
- setting 47, 782

IPv6

- displaying neighbors 813
- enabling 800
- MTU 801

IPv6 address

- dynamic configuration (global unicast) 795
- dynamic configuration (link-local) 52, 800
- EUI format 797
- EUI-64 setting 797
- explicit configuration 800
- global unicast 794
- link-local 796
- manual configuration (global unicast) 48, 794
- manual configuration (link-local) 48, 799
- setting 47, 794

IPv6 source guard

- configuring static entries 322
- setting maximum bindings 325

## J

jumbo frame 102

## K

key

- private 235
- public 235
- user public, importing 105, 109

key pair

- host 235
- host, generating 241

## L

LACP

- configuration 401
- group attributes, configuring 409
- group members, configuring 405
- local parameters 411
- partner parameters 411

- protocol message statistics 411
  - protocol parameters 401
  - timeout, for LACPDU 410
- last member query count, IGMP snooping 589
- last member query interval, IGMP snooping 590
- layer 2, protocol tunnel 501
- license information, GNU 823
- Link Layer Discovery Protocol *See* LLDP
- link trace cache, CFM 735, 736, 738
- link trace message, CFM 705, 734, 735, 736
- link type, STA 458
- LLDP 681
  - device statistics details, displaying 703
  - device statistics, displaying 703
  - display device information 701
  - displaying remote information 701
  - interface attributes, configuring 687–698
  - local device information, displaying 700
  - message attributes 681
  - message statistics 703
  - remote information, displaying 701
  - remote port information, displaying 701
  - timing attributes, configuring 683–686
  - TLV, 802.1 690–691
  - TLV, 802.3 692–693
  - TLV, basic 687–689
  - TLV, management address 687
  - TLV, port description 688
  - TLV, system capabilities 688
  - TLV, system description 689
  - TLV, system name 689
- LLDP-MED 681
  - notification, status 695
  - TLV 681
  - TLV, inventory 696
  - TLV, location 694, 697
  - TLV, MED capabilities 697
  - TLV, network policy 698
- local engine ID 171
- logging
  - messages, displaying 132
  - syslog traps 131
  - to syslog servers 129
- logon authentication 201
  - encryption keys 210, 213
  - RADIUS client 208
  - RADIUS server 208
  - sequence 206, 207
  - settings 207
  - TACACS+ client 212
  - TACACS+ server 212
- loop back messages, CFM 705, 739
- loopback detection
  - non-STA 429

- STA 458

## M

- MAC address authentication 273
  - ports, configuring 273, 279
  - reauthentication 275
- MAC address, mirroring 415
- maintenance association, CFM 705, 714, 720
- maintenance domain, CFM 705, 711, 720
- maintenance end point, CFM 712, 716, 721
- maintenance intermediate point, CFM 711, 712, 714, 721
- maintenance level, CFM 711
- maintenance point, CFM 705, 721
- management access, filtering per address 257
- management access, IP filter 257
- matching class settings, classifying QoS traffic 568
- mDNS
  - domain name list 767
  - enabling lookup 767
  - multicast name service 767
  - name server list 767
- media-type 377
- memory
  - status 92
  - utilization, showing 92
- memory utilization, setting trap 182
- MEP archive, CFM 728
- mirror port
  - configuring 415
  - configuring local traffic 415
  - configuring remote traffic 418
- MLD
  - filter profiles, configuration 632
  - filtering & throttling 631
  - filtering & throttling, configuring profile 633
  - filtering & throttling, creating profile 632
  - filtering & throttling, enabling 631
  - filtering & throttling, interface configuration 634–635
  - filtering & throttling, status 631
- MLD snooping 614
  - configuring 614
  - enabling 615
  - immediate leave 621
  - immediate leave, status 621
  - multicast static router port 622
  - querier 616
  - querier, enabling 616
  - query interval 617
  - query, maximum response time 617
  - robustness value 618
  - static port assignment 623
  - static router port 622
  - unknown multicast, handling 619
  - version 620



## Index

- MSTP 446
    - global settings, configuring 441
    - global settings, displaying 469
    - interface settings, configuring 442, 454–466
    - interface settings, displaying 468
    - path cost 462
  - MTU for IPv6 801
  - Multicast Domain Name Service *See* mDNS
  - multicast filtering 577
    - enabling IGMP snooping 579
    - enabling IGMP snooping per interface 579
    - enabling MLD snooping 615
    - router configuration 601
  - multicast groups 597
    - static 594, 597
  - Multicast Listener Discovery *See* MLD snooping
  - multicast router discovery 590
  - multicast router port, displaying 598
  - multicast services
    - configuring 594
    - displaying 597
  - multicast static router port 601
    - configuring 601
    - configuring for MLD snooping 622
  - multicast storm, threshold 427
  - multicast, filtering and throttling 603, 631
  - MVR
    - assigning static multicast groups 643, 651
    - configuring 640, 648
    - interface status, configuring 649–651
    - interface status, displaying 653
    - IP for control packets sent upstream 647
    - proxy query interval 644
    - proxy switching 645
    - receiver groups, displaying 655
    - robust value for proxy switching 646
    - setting interface type 650
    - setting multicast domain 642
    - setting multicast groups 641, 643
    - setting multicast priority 643, 664
    - source port mode 647
    - specifying a domain 642
    - specifying a VLAN 641, 648
    - specifying priority 643, 664
    - static binding 643, 651
    - static binding, group to port 651
    - statistics, displaying 658
    - using immediate leave 649
  - MVR6
    - assigning static multicast groups 665, 672
    - configuring 662, 669
    - interface status, configuring 670–672
    - interface status, displaying 676
    - IP for control packets sent upstream 669
    - proxy query interval 644
    - proxy switching 666
    - receiver groups, displaying 677
    - robust value for proxy switching 667
    - setting interface type 671
    - setting multicast domain 663
    - setting multicast groups 665
    - setting multicast priority 664
    - source port mode 647
    - specifying a domain 663
    - specifying a VLAN 669
    - specifying priority 664
    - static binding 665, 672
    - static binding, group to port 672
    - statistics, displaying 679
    - using immediate leave 670
- ## N
- network access
    - authentication 273
    - dynamic QoS assignment 276
    - dynamic VLAN assignment 277
    - MAC address filter 274
    - port configuration 279
    - reauthentication 275
    - secure MAC information 283, 284
  - NTP
    - authentication keys, specifying 142
    - client, enabling 143
    - specifying servers 144
  - NTP, setting the system clock 142–145
- ## O
- ### OAM
- active mode 751
  - displaying settings and status 755–758
  - enabling on switch ports 748
  - errored frame link events 749–750
  - event log, displaying 755
  - message statistics, displaying 755
  - mode selection 751
  - passive mode 751
  - remote device information, displaying 758
  - remote loop back test 754
  - setting to active mode 751
  - setting to passive mode 751
- Operations, Administration and Maintenance *See* OAM
- ## P
- password, line 121
  - passwords 45, 202
    - administrator setting 203



- path cost 456
  - method 447
  - STA 447, 456
- policy map
  - description 567
  - DiffServ 570
- port authentication 245, 246
- port priority
  - configuring 553
  - default ingress 556
  - STA 464
- port security, configuring 268
- port, statistics 381
- ports
  - autonegotiation 377
  - broadcast storm threshold 427
  - capabilities 373
  - configuring 371
  - discard CDP/PVST 375
  - duplex mode 379
  - flow control 375
  - forced selection of media type 377
  - forced selection on combo ports 377
  - mirroring 415
  - mirroring local traffic 415
  - mirroring remote traffic 418
  - multicast storm threshold 427
  - speed 379
  - statistics 381
  - unknown unicast storm threshold 427
- power savings
  - configuring 399
  - enabling per port 399
- PPPoE 259–265
- priority, default port ingress 556
- private key 235
- privilege level, defining per command 205
- problems, troubleshooting 821
- protocol migration 467
- protocol tunnel, layer 2 501
- protocol VLANs 504
  - configuring 505, 506
  - interface configuration 506
  - system configuration 505
- proxy ARP 790
- proxy query address, IGMP snooping 591
- proxy query interval, IGMP snooping 593
- proxy query response interval, IGMP snooping 593
- proxy reporting, IGMP snooping 580, 615
- public key 235
- PVID, port native VLAN 486
- PVST, discard 375

## Q

- QoS 565
  - configuration guidelines 566
  - configuring 565
  - dynamic assignment 276
  - matching class settings 568
  - selecting DSCP, CoS 561
- QoS policy, committed information rate 571
- queue weight, assigning to CoS 555

## R

- RADIUS
  - logon authentication 208
  - settings 208
- rate limit
  - port 426
  - setting 425
- remote engine ID 171
- remote logging 131
- remote maintenance end point, CFM 722, 723, 728, 732
- Remote Monitoring *See* RMON
- rename, DiffServ 569
- restarting the system 82, 86
  - at scheduled times 82
  - showing restart time 87
- RMON 187
  - alarm, displaying settings 192
  - alarm, setting thresholds 188
  - commands 187
  - event settings, displaying 192
  - response to alarm setting 189
  - statistics history, collection 190
  - statistics history, displaying 193
  - statistics, collection 191
  - statistics, displaying 193
- routing information base, description 817
- routing table, displaying 817
- RSA encryption 241
- RSTP 446
  - global settings, configuring 446
  - global settings, displaying 468
  - interface settings, configuring 454–466
  - interface settings, displaying 468
- running configuration files, displaying 96

## S

- secure shell 235
  - configuration 236
- security, general measures 267
- serial port, configuring 116
- service instance, CFM 714

## Index

- sFlow
    - destination for traffic 195
    - destination, IPv6 196
    - destination, UDP port 196
    - flow configuration 195–199
    - initiating 198
    - maximum datagram size 196
    - owner 195
    - polling period 197
    - sampling period 198
    - timeout 195
    - version 196
  - SMTP
    - event handling 134
    - sending log events 134
  - SNMP 161
    - community string 163
    - enabling traps 166
    - enabling traps, mac-address changes 170
    - filtering IP addresses 257
    - global settings, configuring 163–175
    - mac address traps 166, 170
    - trap manager 167
    - traps, CFM 727, 731
  - SNMPv3 171–173
    - engine ID 171
    - engine identifier, local 171
    - engine identifier, remote 171
    - groups 172
    - local users, configuring 173
    - remote users, configuring 173
    - user configuration 173
    - views 175
  - SNTP
    - setting the system clock 139–141
    - specifying servers 140
  - software
    - displaying version 101
    - downloading 105
    - version, displaying 101
  - SSH 235
    - authentication retries 238
    - configuring 236
    - downloading public keys for clients 105, 109
    - generating host key pair 241
    - server, configuring 238
    - timeout 240
  - STA 441
    - BPDU filter 454
    - BPDU flooding 463
    - BPDU shutdown 455
    - cisco-prestandard, setting compatibility 443
    - detecting loopbacks 458
    - edge port 457
    - global settings, configuring 442–450
    - global settings, displaying 468
    - interface settings, configuring 454–466
    - interface settings, displaying 469
    - link type 458
    - loopback detection 458
    - MSTP interface settings, configuring 451–453
    - MSTP path cost 462
    - path cost 447, 456
    - path cost method 447
    - port priority 464
    - port/trunk loopback detection 458
    - protocol migration 467
    - transmission limit 450
  - startup files
    - creating 105
    - displaying 97, 111
    - setting 104
  - static addresses, setting 436
  - static routes, configuring 816
  - statistics
    - ARP 786
    - ICMP 786
    - IP 786
    - TCP 786
    - UDP 786
  - statistics, port 381
  - STP 446
    - Also see STA*
  - summary, accounting 226
  - summer time, setting 145–148
  - switch clustering, for management 154
  - switch settings
    - restoring 103
    - saving 103
  - system clock
    - setting 138
    - setting manually 150
    - setting the time zone 149
    - setting with NTP 142–145
    - setting with SNTP 139–141
    - summer time 145–148
  - system clock, setting 64
  - system logs 130
  - system software, downloading from server 105
- ## T
- TACACS+
    - logon authentication 212
    - settings 212
  - TCN
    - flood 583
    - general query solicitation 584

- Telnet
  - configuring 232
  - server, enabling 234
- terminal, configuration settings 125
- TFTP
  - retry count 114
  - timeout 115
- time range, ACL 151
- time zone, setting 149
- time, setting 138
- TPID 495
- traffic segmentation 341
  - assigning ports 343
  - enabling 342
  - sessions, assigning ports 343
  - sessions, creating 343
- transceiver thresholds
  - displaying 396
- trap manager 54, 167
- troubleshooting 821
- trunk
  - configuration 401
  - LACP 401, 405
  - load balancing 402
  - static 404
- protocol, interface configuration 506
- protocol, system configuration 505
- PVID 486
- tag swapping 502
- voice 512
- voice VLANs 512
  - detecting VoIP devices 513
  - enabling for ports 516
  - identifying client devices 515
- VoIP traffic 512
  - ports, configuring 516
  - telephony OUI, configuring 515
  - voice VLAN, configuring 512
- VoIP, detecting devices 517

## W

- web authentication 287
  - address, re-authenticating 288
  - configuring 287
  - configuring ports 287
  - port information, displaying 289
  - ports, configuring 287
  - ports, re-authenticating 288

## U

- unicast routing 815
- unknown unicast storm, threshold 427
- unregistered data flooding, IGMP snooping 585
- upgrading software 105, 111
- user account 202, 203
- user password 202, 203

## V

- VLANs 473–518
  - 802.1Q tunnel mode 490
  - acceptable frame type 483
  - adding static members 483
  - basic information, displaying 477
  - creating 480
  - displaying port members 487
  - dynamic assignment 277
  - egress mode 485
  - ingress filtering 485
  - interface configuration 483–486
  - IP subnet-based 508
  - MAC-based 510
  - mirroring 415
  - port members, displaying 487
  - protocol 504
  - protocol, configuring 505, 506
  - protocol, configuring groups 505

