



ECS4510-28T/P/F
ECS4510-52T/P
28/52-Port Layer 2+
Gigabit Ethernet Switch

Management Guide

ECS4510-28T GIGABIT ETHERNET SWITCH

*Layer 2+ Gigabit Ethernet Switch
with 24 10/100/1000BASE-T (RJ-45) Ports,
2 10-Gigabit SFP+ Ports,
and Optional Module with 2 10-Gigabit SFP+ Ports*

ECS4510-28P GIGABIT ETHERNET PoE SWITCH

*Layer 2+ Gigabit Ethernet PoE Switch
with 24 10/100/1000BASE-T (RJ-45) Ports,
2 10-Gigabit SFP+ Ports,
and Optional Module with 2 10-Gigabit SFP+ Ports*

ECS4510-28F GIGABIT ETHERNET FIBER SWITCH

*Layer 2+ Gigabit Ethernet Fiber Switch
with 22 SFP Ports,
with 2 10/100/1000BASE-T (RJ-45/SFP) Ports,
2 10-Gigabit SFP+ Ports,
and Optional Module with 2 10-Gigabit SFP+ Ports*

ECS4510-52T GIGABIT ETHERNET SWITCH

*Layer 2+ Gigabit Ethernet Switch
with 48 10/100/1000BASE-T (RJ-45) Ports,
2 10-Gigabit SFP+ Ports,
and Optional Module with 2 10-Gigabit SFP+ Ports*

ECS4510-52P GIGABIT ETHERNET PoE SWITCH

*Layer 2+ Gigabit Ethernet PoE Switch
with 48 10/100/1000BASE-T (RJ-45) Ports,
2 10-Gigabit SFP+ Ports,
and Optional Module with 2 10-Gigabit SFP+ Ports*

E052013/ST-R04

ECS4510-28T	149100000189A
ECS4510-28P	149100000189A
ECS4510-28F	149100000189A
ECS4510-52T	149100000191A
ECS4510-52P	149100000191A

ABOUT THIS GUIDE

PURPOSE This guide gives specific information on how to operate and use the management functions of the switch.

AUDIENCE The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

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.



WARNING: Alerts you to a potential hazard that could cause personal injury.

RELATED PUBLICATIONS The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch:

The Installation Guide

Also, as part of the switch's software, there is an online web-based help that describes all management related features.

REVISION HISTORY This section summarizes the changes in each revision of this guide.

MAY 2013 REVISION

This is the fourth version of this guide. This guide is valid for software release v1.3.2.1. This release adds support for the ECS4510-52P.

DECEMBER 2012 REVISION

This is the third version of this guide. This guide is valid for software release v1.3.1.7. This release adds support for Layer 3 lite, including static and dynamic routing. It also includes information on the following changes:

- ◆ Added support for ECS4510-52T. (See [Figure 2, "Front Panel Indicators," on page 101.](#))
- ◆ Updated description for ["Setting an IP Address" on page 83.](#)
- ◆ Added "L3 Interface" parameter to the static VLAN configuration pages. (See ["Configuring VLAN Groups" on page 196.](#))
- ◆ Updated default settings for storm control rate limit. (See ["Storm Control" on page 260.](#))
- ◆ Changed method of configuring an IPv4 address to follow conventions for a Layer 3 switch. (See ["Setting the Switch's IP Address \(IP Version 4\)" on page 617.](#))
- ◆ Removed DHCP Relay Option 82 as an unsupported Layer 2 feature. This switch now only supports configuring the address for relay servers. (See ["Configuring DHCP Relay Service" on page 647](#) and ["DHCP Relay" on page 1364.](#))
- ◆ Added a chapter describing the general commands for Layer 3 lite functions, including IP interface configuration, configuring static routes, and displaying the routing table. (See ["General IP Routing" on page 655.](#))
- ◆ Added trace route function (See ["Using the Trace Route Function" on page 660.](#))
- ◆ Added chapter on unicast routing, including description of general routing and the Routing Information Protocol. (See ["Unicast Routing" on page 671.](#))
- ◆ Added the command ["terminal" on page 755.](#)
- ◆ Updated description of the command ["interface" on page 974.](#)
- ◆ Change configuration mode to VLAN interface for ["ip dhcp relay server" on page 1364.](#)
- ◆ Added max-failures parameter to ["traceroute6" on page 1397.](#)
- ◆ Added the command ["ipv6 hop-limit" on page 1398.](#)

SEPTEMBER 2012 REVISION

This is the second version of this guide. This guide is valid for software release v1.2.2.0. It includes information on the following changes:

- ◆ Added support for ECS4510-28F and ECS4510-28P. (See [Figure 2, "Front Panel Indicators," on page 101.](#))
- ◆ Added "Media Type" to Parameter list under ["Configuring by Port List" on page 151.](#)
- ◆ Added "Timeout Mode" to Parameter list under ["Configuring a Dynamic Trunk" on page 172.](#)
- ◆ Updated information on maximum ACL rules in the Command Usage section under ["Access Control Lists" on page 347.](#)
- ◆ Added description of LLDP-MED TLVs reported by end-node devices in the Parameters section under ["Displaying LLDP Remote Device Information" on page 428.](#)
- ◆ Added ["Power over Ethernet" on page 438](#) for the ECS4510-28P.
- ◆ Added support for ERPSv2 as described under ["Ethernet Ring Protection Switching" on page 485.](#)
- ◆ Added more information for DHCP Option 60, 66 and 67 statements in the Command Usage section under ["Specifying A DHCP Client Identifier" on page 645.](#)
- ◆ Added support for PPPoE IA as described under ["Configuring the PPPoE Intermediate Agent" on page 648.](#)
- ◆ Added ["TFTP Configuration Commands" on page 744.](#)
- ◆ Added PPPoE IA configuration commands as described under ["PPPoE Intermediate Agent" on page 879.](#)
- ◆ Added [lacp timeout](#) command on [page 1001.](#)
- ◆ Added ["Power over Ethernet Commands" on page 1007.](#)
- ◆ Added commands for ERPSv2, including ["non-revertive" on page 1097,](#) ["raps-def-mac" on page 1102,](#) ["raps-without-vc" on page 1102,](#) ["rpl neighbor" on page 1105,](#) ["rpl neighbor" on page 1105,](#) ["version" on page 1107,](#) ["clear erps statistics" on page 1108,](#) ["erps clear" on page 1109,](#) ["erps forced-switch" on page 1109,](#) and ["erps manual-switch" on page 1111.](#)
- ◆ Added [lldp dot3-tlv poe](#) and [lldp med-tlv ext-poe](#) commands on [page 1282](#) and [page 1285,](#) respectively for the ECS4510-28P.
- ◆ Added more information for DHCP Option 60, 66 and 67 statements in the Command Usage section under the [ip dhcp client class-id](#) command on [page 1358.](#)

MAY 2012 REVISION

This is the first version of this guide. This guide is valid for software release v1.1.2.1.

CONTENTS

ABOUT THIS GUIDE	5
CONTENTS	9
FIGURES	47
TABLES	61

SECTION I	GETTING STARTED	67
1	INTRODUCTION	69
	Key Features	69
	Description of Software Features	70
	IP Routing	74
	Address Resolution Protocol	75
	System Defaults	76
2	INITIAL SWITCH CONFIGURATION	79
	Connecting to the Switch	79
	Configuration Options	79
	Required Connections	80
	Remote Connections	81
	Basic Configuration	82
	Console Connection	82
	Setting Passwords	82
	Setting an IP Address	83
	Downloading a Configuration File Referenced by a DHCP Server	90
	Enabling SNMP Management Access	92
	Managing System Files	94
	Saving or Restoring Configuration Settings	95

SECTION II	WEB CONFIGURATION	97
3	USING THE WEB INTERFACE	99
	Connecting to the Web Interface	99
	Navigating the Web Browser Interface	100
	Home Page	100
	Configuration Options	101
	Panel Display	101
	Main Menu	102
4	BASIC MANAGEMENT TASKS	119
	Displaying System Information	120
	Displaying Hardware/Software Versions	121
	Configuring Support for Jumbo Frames	122
	Displaying Bridge Extension Capabilities	123
	Managing System Files	125
	Copying Files via FTP/TFTP or HTTP	125
	Saving the Running Configuration to a Local File	127
	Setting The Start-Up File	128
	Showing System Files	129
	Automatic Operation Code Upgrade	130
	Setting the System Clock	134
	Setting the Time Manually	134
	Setting the SNTP Polling Interval	135
	Configuring NTP	136
	Configuring Time Servers	137
	Setting the Time Zone	141
	Configuring the Console Port	142
	Configuring Telnet Settings	144
	Displaying CPU Utilization	145
	Displaying Memory Utilization	146
	Resetting the System	147
5	INTERFACE CONFIGURATION	151
	Port Configuration	151
	Configuring by Port List	151
	Configuring by Port Range	154
	Displaying Connection Status	155

Configuring Local Port Mirroring	156
Configuring Remote Port Mirroring	158
Showing Port or Trunk Statistics	162
Performing Cable Diagnostics	166
Trunk Configuration	168
Configuring a Static Trunk	169
Configuring a Dynamic Trunk	172
Displaying LACP Port Counters	178
Displaying LACP Settings and Status for the Local Side	179
Displaying LACP Settings and Status for the Remote Side	181
Saving Power	182
Sampling Traffic Flows	184
Configuring sFlow Global Settings	185
Configuring sFlow Interface Settings	185
Traffic Segmentation	187
Enabling Traffic Segmentation	187
Configuring Uplink and Downlink Ports	189
VLAN Trunking	191
6 VLAN CONFIGURATION	193
IEEE 802.1Q VLANs	193
Configuring VLAN Groups	196
Adding Static Members to VLANs	199
Configuring Dynamic VLAN Registration	203
IEEE 802.1Q Tunneling	206
Enabling QinQ Tunneling on the Switch	210
Creating CVLAN to SPVLAN Mapping Entries	211
Adding an Interface to a QinQ Tunnel	213
Protocol VLANs	215
Configuring Protocol VLAN Groups	215
Mapping Protocol Groups to Interfaces	217
Configuring IP Subnet VLANs	219
Configuring MAC-based VLANs	221
Configuring VLAN Mirroring	223
Configuring VLAN Translation	224
7 ADDRESS TABLE SETTINGS	227
Setting Static Addresses	227

Changing the Aging Time	229
Displaying the Dynamic Address Table	230
Clearing the Dynamic Address Table	231
Configuring MAC Address Mirroring	232
8 SPANNING TREE ALGORITHM	235
Overview	235
Configuring Loopback Detection	238
Configuring Global Settings for STA	240
Displaying Global Settings for STA	245
Configuring Interface Settings for STA	246
Displaying Interface Settings for STA	250
Configuring Multiple Spanning Trees	253
Configuring Interface Settings for MSTP	257
9 CONGESTION CONTROL	259
Rate Limiting	259
Storm Control	260
Automatic Traffic Control	263
Setting the ATC Timers	264
Configuring ATC Thresholds and Responses	266
10 CLASS OF SERVICE	269
Layer 2 Queue Settings	269
Setting the Default Priority for Interfaces	269
Selecting the Queue Mode	270
Mapping CoS Values to Egress Queues	273
Layer 3/4 Priority Settings	276
Setting Priority Processing to DSCP or CoS	276
Mapping Ingress DSCP Values to Internal DSCP Values	277
Mapping CoS Priorities to Internal DSCP Values	280
11 QUALITY OF SERVICE	283
Overview	283
Configuring a Class Map	284
Creating QoS Policies	287
Attaching a Policy Map to a Port	297
12 VOIP TRAFFIC CONFIGURATION	299
Overview	299
Configuring VoIP Traffic	299

Configuring Telephony OUI	301
Configuring VoIP Traffic Ports	302
13 SECURITY MEASURES	305
AAA (Authentication, Authorization and Accounting)	306
Configuring Local/Remote Logon Authentication	307
Configuring Remote Logon Authentication Servers	308
Configuring AAA Accounting	313
Configuring AAA Authorization	319
Configuring User Accounts	322
Web Authentication	324
Configuring Global Settings for Web Authentication	324
Configuring Interface Settings for Web Authentication	325
Network Access (MAC Address Authentication)	326
Configuring Global Settings for Network Access	329
Configuring Network Access for Ports	330
Configuring Port Link Detection	332
Configuring a MAC Address Filter	333
Displaying Secure MAC Address Information	335
Configuring HTTPS	336
Configuring Global Settings for HTTPS	336
Replacing the Default Secure-site Certificate	338
Configuring the Secure Shell	340
Configuring the SSH Server	342
Generating the Host Key Pair	344
Importing User Public Keys	345
Access Control Lists	347
Setting A Time Range	349
Showing TCAM Utilization	351
Setting the ACL Name and Type	352
Configuring a Standard IPv4 ACL	354
Configuring an Extended IPv4 ACL	356
Configuring a Standard IPv6 ACL	358
Configuring an Extended IPv6 ACL	360
Configuring a MAC ACL	362
Configuring an ARP ACL	364
Binding a Port to an Access Control List	366

Configuring ACL Mirroring	367
Showing ACL Hardware Counters	369
ARP Inspection	370
Configuring Global Settings for ARP Inspection	371
Configuring VLAN Settings for ARP Inspection	373
Configuring Interface Settings for ARP Inspection	375
Displaying ARP Inspection Statistics	376
Displaying the ARP Inspection Log	377
Filtering IP Addresses for Management Access	378
Configuring Port Security	380
Configuring 802.1X Port Authentication	382
Configuring 802.1X Global Settings	384
Configuring Port Authenticator Settings for 802.1X	385
Configuring Port Supplicant Settings for 802.1X	389
Displaying 802.1X Statistics	391
DoS Protection	394
IP Source Guard	396
Configuring Ports for IP Source Guard	397
Configuring Static Bindings for IP Source Guard	399
Displaying Information for Dynamic IP Source Guard Bindings	401
DHCP Snooping	402
DHCP Snooping Configuration	404
DHCP Snooping VLAN Configuration	406
Configuring Ports for DHCP Snooping	407
Displaying DHCP Snooping Binding Information	408
14 BASIC ADMINISTRATION PROTOCOLS	411
Configuring Event Logging	412
System Log Configuration	412
Remote Log Configuration	414
Sending Simple Mail Transfer Protocol Alerts	415
Link Layer Discovery Protocol	416
Setting LLDP Timing Attributes	417
Configuring LLDP Interface Attributes	419
Configuring LLDP Interface Civic-Address	422
Displaying LLDP Local Device Information	424
Displaying LLDP Remote Device Information	428

Displaying Device Statistics	436
Power over Ethernet	438
Displaying the Switch's Overall PoE Power Budget	439
Setting The Port PoE Power Budget	440
Simple Network Management Protocol	442
Configuring Global Settings for SNMP	444
Setting the Local Engine ID	445
Specifying a Remote Engine ID	446
Setting SNMPv3 Views	448
Configuring SNMPv3 Groups	451
Setting Community Access Strings	456
Configuring Local SNMPv3 Users	457
Configuring Remote SNMPv3 Users	459
Specifying Trap Managers	462
Creating SNMP Notification Logs	466
Showing SNMP Statistics	468
Remote Monitoring	470
Configuring RMON Alarms	471
Configuring RMON Events	473
Configuring RMON History Samples	475
Configuring RMON Statistical Samples	478
Switch Clustering	481
Configuring General Settings for Clusters	481
Cluster Member Configuration	483
Managing Cluster Members	484
Ethernet Ring Protection Switching	485
ERPS Global Configuration	489
ERPS Ring Configuration	490
ERPS Forced and Manual Mode Operations	506
Connectivity Fault Management	510
Configuring Global Settings for CFM	513
Configuring Interfaces for CFM	517
Configuring CFM Maintenance Domains	517
Configuring CFM Maintenance Associations	522
Configuring Maintenance End Points	527
Configuring Remote Maintenance End Points	528

Transmitting Link Trace Messages	530
Transmitting Loop Back Messages	532
Transmitting Delay-Measure Requests	534
Displaying Local MEPs	536
Displaying Details for Local MEPs	537
Displaying Local MIPs	539
Displaying Remote MEPs	540
Displaying Details for Remote MEPs	541
Displaying the Link Trace Cache	543
Displaying Fault Notification Settings	544
Displaying Continuity Check Errors	545
OAM Configuration	547
Enabling OAM on Local Ports	547
Displaying Statistics for OAM Messages	549
Displaying the OAM Event Log	550
Displaying the Status of Remote Interfaces	551
Configuring a Remote Loop Back Test	552
Displaying Results of Remote Loop Back Testing	554
15 MULTICAST FILTERING	557
Overview	557
Layer 2 IGMP (Snooping and Query)	558
Configuring IGMP Snooping and Query Parameters	560
Specifying Static Interfaces for a Multicast Router	564
Assigning Interfaces to Multicast Services	566
Setting IGMP Snooping Status per Interface	568
Filtering IGMP Query Packets and Multicast Data	573
Displaying Multicast Groups Discovered by IGMP Snooping	574
Displaying IGMP Snooping Statistics	575
Filtering and Throttling IGMP Groups	579
Enabling IGMP Filtering and Throttling	579
Configuring IGMP Filter Profiles	580
Configuring IGMP Filtering and Throttling for Interfaces	582
Multicast VLAN Registration for IPv4	584
Configuring MVR Global Settings	585
Configuring MVR Domain Settings	587
Configuring MVR Group Address Profiles	589

Configuring MVR Interface Status	592
Assigning Static MVR Multicast Groups to Interfaces	594
Displaying MVR Receiver Groups	596
Displaying MVR Statistics	597
Multicast VLAN Registration for IPv6	601
Configuring MVR6 Global Settings	602
Configuring MVR6 Domain Settings	604
Configuring MVR6 Group Address Profiles	605
Configuring MVR6 Interface Status	608
Assigning Static MVR6 Multicast Groups to Interfaces	610
Displaying MVR6 Receiver Groups	612
Displaying MVR6 Statistics	613
16 IP CONFIGURATION	617
Setting the Switch's IP Address (IP Version 4)	617
Setting the Switch's IP Address (IP Version 6)	621
Configuring the IPv6 Default Gateway	621
Configuring IPv6 Interface Settings	622
Configuring an IPv6 Address	627
Showing IPv6 Addresses	630
Showing the IPv6 Neighbor Cache	631
Showing IPv6 Statistics	633
Showing the MTU for Responding Destinations	638
17 IP SERVICES	639
Domain Name Service	639
Configuring General DNS Service Parameters	639
Configuring a List of Domain Names	640
Configuring a List of Name Servers	642
Configuring Static DNS Host to Address Entries	643
Displaying the DNS Cache	644
Dynamic Host Configuration Protocol	645
Specifying A DHCP Client Identifier	645
Configuring DHCP Relay Service	647
Configuring the PPPoE Intermediate Agent	648
Configuring PPPoE IA Global Settings	648
Configuring PPPoE IA Interface Settings	650
Showing PPPoE IA Statistics	652

18 GENERAL IP ROUTING	655
Overview	655
Initial Configuration	655
IP Routing and Switching	656
Routing Path Management	657
Routing Protocols	658
Configuring IP Routing Interfaces	658
Configuring Local and Remote Interfaces	658
Using the Ping Function	659
Using the Trace Route Function	660
Address Resolution Protocol	661
Basic ARP Configuration	662
Configuring Static ARP Addresses	664
Displaying Dynamic or Local ARP Entries	665
Displaying ARP Statistics	666
Configuring Static Routes	667
Displaying the Routing Table	669
19 UNICAST ROUTING	671
Overview	671
Configuring the Routing Information Protocol	672
Configuring General Protocol Settings	673
Clearing Entries from the Routing Table	676
Specifying Network Interfaces	677
Specifying Passive Interfaces	679
Specifying Static Neighbors	680
Configuring Route Redistribution	681
Specifying an Administrative Distance	683
Configuring Network Interfaces for RIP	685
Displaying RIP Interface Settings	689
Displaying Peer Router Information	689
Resetting RIP Statistics	690

SECTION III	COMMAND LINE INTERFACE	691
20	USING THE COMMAND LINE INTERFACE	693
	Accessing the CLI	693
	Console Connection	693
	Telnet Connection	694
	Entering Commands	695
	Keywords and Arguments	695
	Minimum Abbreviation	695
	Command Completion	695
	Getting Help on Commands	696
	Partial Keyword Lookup	698
	Negating the Effect of Commands	698
	Using Command History	698
	Understanding Command Modes	698
	Exec Commands	699
	Configuration Commands	700
	Command Line Processing	702
	Showing Status Information	702
	CLI Command Groups	703
21	GENERAL COMMANDS	707
	prompt	707
	reload (Global Configuration)	708
	enable	709
	quit	710
	show history	710
	configure	711
	disable	712
	reload (Privileged Exec)	712
	show reload	713
	end	713
	exit	713
22	SYSTEM MANAGEMENT COMMANDS	715
	Device Designation	715
	hostname	716

Banner Information	716
banner configure	717
banner configure company	718
banner configure dc-power-info	719
banner configure department	719
banner configure equipment-info	720
banner configure equipment-location	721
banner configure ip-lan	721
banner configure ip-number	722
banner configure manager-info	723
banner configure mux	723
banner configure note	724
show banner	725
System Status	725
show access-list tcam-utilization	726
show memory	726
show process cpu	727
show running-config	727
show startup-config	729
show system	729
show tech-support	730
show users	731
show version	732
show watchdog	732
watchdog software	732
Frame Size	733
jumbo frame	733
File Management	734
General Commands	735
boot system	735
copy	736
delete	739
dir	739
whichboot	740
Automatic Code Upgrade Commands	741
upgrade opcode auto	741

upgrade opcode path	742
upgrade opcode reload	743
show upgrade	744
TFTP Configuration Commands	744
ip tftp retry	744
ip tftp timeout	745
show ip tftp	745
Line	746
line	747
databits	747
exec-timeout	748
login	749
parity	750
password	750
password-thresh	751
silent-time	752
speed	752
stopbits	753
timeout login response	754
disconnect	754
terminal	755
show line	756
Event Logging	757
logging facility	757
logging history	758
logging host	759
logging on	759
logging trap	760
clear log	760
show log	761
show logging	762
SMTP Alerts	763
logging sendmail	764
logging sendmail host	764
logging sendmail level	765
logging sendmail destination-email	765

logging sendmail source-email	766
show logging sendmail	766
Time	767
SNTP Commands	768
sntp client	768
sntp poll	769
sntp server	769
show sntp	770
NTP Commands	770
ntp authenticate	770
ntp authentication-key	771
ntp client	772
ntp server	773
show ntp	774
Manual Configuration Commands	774
clock timezone	774
calendar set	775
show calendar	776
Time Range	776
time-range	776
absolute	777
periodic	778
show time-range	779
Switch Clustering	779
cluster	780
cluster commander	781
cluster ip-pool	781
cluster member	782
rcommand	783
show cluster	783
show cluster members	784
show cluster candidates	784
23 SNMP COMMANDS	785
General SNMP Commands	787
snmp-server	787
snmp-server community	787

snmp-server contact	788
snmp-server location	788
show snmp	789
SNMP Target Host Commands	790
snmp-server enable traps	790
snmp-server host	791
SNMPv3 Commands	793
snmp-server engine-id	793
snmp-server group	794
snmp-server user	795
snmp-server view	797
show snmp engine-id	798
show snmp group	798
show snmp user	799
show snmp view	800
Notification Log Commands	801
nlm	801
snmp-server notify-filter	801
show nlm oper-status	803
show snmp notify-filter	803
Additional Trap Commands	803
memory	803
process cpu	804
24 REMOTE MONITORING COMMANDS	807
rmon alarm	808
rmon event	809
rmon collection history	810
rmon collection rmon1	811
show rmon alarms	812
show rmon events	812
show rmon history	812
show rmon statistics	813
25 FLOW SAMPLING COMMANDS	815
sflow	815
sflow destination	816
sflow max-datagram-size	817

sflow max-header-size	817
sflow owner	818
sflow polling-interval	818
sflow sample	819
sflow source	819
sflow timeout	820
show sflow	820
26 AUTHENTICATION COMMANDS	823
User Accounts and Privilege Levels	824
enable password	824
username	825
privilege	826
show privilege	827
Authentication Sequence	827
authentication enable	828
authentication login	829
RADIUS Client	830
radius-server acct-port	830
radius-server auth-port	831
radius-server host	831
radius-server key	832
radius-server retransmit	832
radius-server timeout	833
show radius-server	833
TACACS+ Client	834
tacacs-server host	834
tacacs-server key	835
tacacs-server port	836
tacacs-server retransmit	836
tacacs-server timeout	837
show tacacs-server	837
AAA	838
aaa accounting commands	838
aaa accounting dot1x	839
aaa accounting exec	840
aaa accounting update	841

aaa authorization exec	842
aaa group server	843
server	843
accounting dot1x	844
accounting commands	844
accounting exec	845
authorization exec	845
show accounting	846
Web Server	847
ip http port	847
ip http server	848
ip http secure-port	848
ip http secure-server	849
Telnet Server	850
ip telnet max-sessions	851
ip telnet port	851
ip telnet server	852
show ip telnet	852
Secure Shell	852
ip ssh authentication-retries	855
ip ssh server	856
ip ssh server-key size	857
ip ssh timeout	857
delete public-key	858
ip ssh crypto host-key generate	858
ip ssh crypto zeroize	859
ip ssh save host-key	860
show ip ssh	860
show public-key	860
show ssh	861
802.1X Port Authentication	862
General Commands	863
dot1x default	863
dot1x eapol-pass-through	863
dot1x system-auth-control	864

Authenticator Commands	864
dot1x intrusion-action	864
dot1x max-reauth-req	865
dot1x max-req	865
dot1x operation-mode	866
dot1x port-control	867
dot1x re-authentication	867
dot1x timeout quiet-period	868
dot1x timeout re-authperiod	868
dot1x timeout supp-timeout	869
dot1x timeout tx-period	870
dot1x re-authenticate	870
Supplicant Commands	871
dot1x identity profile	871
dot1x max-start	871
dot1x pae supplicant	872
dot1x timeout auth-period	873
dot1x timeout held-period	873
dot1x timeout start-period	874
Information Display Commands	874
show dot1x	874
Management IP Filter	877
management	877
show management	878
PPPoE Intermediate Agent	879
pppoe intermediate-agent	879
pppoe intermediate-agent format-type	880
pppoe intermediate-agent port-enable	881
pppoe intermediate-agent port-format-type	881
pppoe intermediate-agent trust	882
pppoe intermediate-agent vendor-tag strip	883
clear pppoe intermediate-agent statistics	883
show pppoe intermediate-agent info	884
show pppoe intermediate-agent statistics	885

27 GENERAL SECURITY MEASURES	887
Port Security	888
port security	888
show port security	890
Network Access (MAC Address Authentication)	892
network-access aging	893
network-access mac-filter	893
mac-authentication reauth-time	894
network-access dynamic-qos	895
network-access dynamic-vlan	896
network-access guest-vlan	897
network-access link-detection	897
network-access link-detection link-down	898
network-access link-detection link-up	898
network-access link-detection link-up-down	899
network-access max-mac-count	899
network-access mode mac-authentication	900
network-access port-mac-filter	901
mac-authentication intrusion-action	902
mac-authentication max-mac-count	902
clear network-access	903
show network-access	903
show network-access mac-address-table	904
show network-access mac-filter	905
Web Authentication	905
web-auth login-attempts	906
web-auth quiet-period	907
web-auth session-timeout	907
web-auth system-auth-control	908
web-auth	908
web-auth re-authenticate (Port)	909
web-auth re-authenticate (IP)	909
show web-auth	910
show web-auth interface	910
show web-auth summary	911

DHCPv4 Snooping	911
ip dhcp snooping	912
ip dhcp snooping information option	914
ip dhcp snooping information policy	915
ip dhcp snooping verify mac-address	916
ip dhcp snooping vlan	917
ip dhcp snooping information option circuit-id	918
ip dhcp snooping trust	919
clear ip dhcp snooping binding	920
clear ip dhcp snooping database flash	920
ip dhcp snooping database flash	921
show ip dhcp snooping	921
show ip dhcp snooping binding	922
DHCPv6 Snooping	922
ipv6 dhcp snooping	922
ipv6 dhcp snooping vlan	925
ipv6 dhcp snooping max-binding	926
ipv6 dhcp snooping trust	926
clear ipv6 dhcp snooping binding	927
clear ipv6 dhcp snooping database flash	928
show ipv6 dhcp snooping	928
show ipv6 dhcp snooping binding	928
show ipv6 dhcp snooping statistics	929
IP Source Guard	929
ip source-guard binding	930
ip source-guard	931
ip source-guard max-binding	933
show ip source-guard	933
show ip source-guard binding	934
ARP Inspection	934
ip arp inspection	935
ip arp inspection filter	936
ip arp inspection log-buffer logs	937
ip arp inspection validate	938
ip arp inspection vlan	939
ip arp inspection limit	940

ip arp inspection trust	940
show ip arp inspection configuration	941
show ip arp inspection interface	941
show ip arp inspection log	942
show ip arp inspection statistics	942
show ip arp inspection vlan	942
Denial of Service Protection	943
dos-protection echo-charge	943
dos-protection smurf	944
dos-protection tcp-flooding	944
dos-protection tcp-null-scan	945
dos-protection tcp-syn-fin-scan	945
dos-protection tcp-xmas-scan	946
dos-protection udp-flooding	946
dos-protection win-nuke	947
show dos-protection	947
28 ACCESS CONTROL LISTS	949
IPv4 ACLs	949
access-list ip	950
permit, deny (Standard IP ACL)	951
permit, deny (Extended IPv4 ACL)	952
ip access-group	954
show ip access-group	955
show ip access-list	955
IPv6 ACLs	956
access-list ipv6	956
permit, deny (Standard IPv6 ACL)	957
permit, deny (Extended IPv6 ACL)	958
show ipv6 access-list	960
ipv6 access-group	961
show ipv6 access-group	961
MAC ACLs	962
access-list mac	962
permit, deny (MAC ACL)	963
mac access-group	965
show mac access-group	966

show mac access-list	966
ARP ACLs	967
access-list arp	967
permit, deny (ARP ACL)	968
show access-list arp	969
ACL Information	969
clear access-list hardware counters	970
show access-group	970
show access-list	970
29 INTERFACE COMMANDS	973
Interface Configuration	974
interface	974
alias	975
capabilities	975
description	976
flowcontrol	977
media-type	978
negotiation	979
shutdown	979
speed-duplex	980
switchport packet-rate	981
clear counters	982
show interfaces brief	983
show interfaces counters	983
show interfaces status	985
show interfaces switchport	986
show interfaces transceiver	987
Cable Diagnostics	988
test cable-diagnostics	988
show cable-diagnostics	989
Power Savings	990
power-save	990
show power-save	991
30 LINK AGGREGATION COMMANDS	993
Manual Configuration Commands	994
port channel load-balance	994

channel-group	996
Dynamic Configuration Commands	996
lacp	996
lacp admin-key (Ethernet Interface)	998
lacp port-priority	999
lacp system-priority	1000
lacp admin-key (Port Channel)	1000
lacp timeout	1001
Trunk Status Display Commands	1002
show lacp	1002
show port-channel load-balance	1005
31 POWER OVER ETHERNET COMMANDS	1007
power inline	1007
power inline maximum allocation	1008
power inline priority	1009
show power inline status	1010
show power mainpower	1011
32 PORT MIRRORING COMMANDS	1013
Local Port Mirroring Commands	1013
port monitor	1013
show port monitor	1015
RSPAN Mirroring Commands	1016
rspan source	1018
rspan destination	1019
rspan remote vlan	1020
no rspan session	1021
show rspan	1022
33 RATE LIMIT COMMANDS	1023
rate-limit	1023
34 AUTOMATIC TRAFFIC CONTROL COMMANDS	1025
Threshold Commands	1028
auto-traffic-control apply-timer	1028
auto-traffic-control release-timer	1028
auto-traffic-control	1029
auto-traffic-control action	1030
auto-traffic-control alarm-clear-threshold	1031

auto-traffic-control alarm-fire-threshold	1032
auto-traffic-control auto-control-release	1033
auto-traffic-control control-release	1033
SNMP Trap Commands	1034
snmp-server enable port-traps atc broadcast-alarm-clear	1034
snmp-server enable port-traps atc broadcast-alarm-fire	1034
snmp-server enable port-traps atc broadcast-control-apply	1035
snmp-server enable port-traps atc broadcast-control-release	1035
snmp-server enable port-traps atc multicast-alarm-clear	1036
snmp-server enable port-traps atc multicast-alarm-fire	1036
snmp-server enable port-traps atc multicast-control-apply	1037
snmp-server enable port-traps atc multicast-control-release	1037
ATC Display Commands	1038
show auto-traffic-control	1038
show auto-traffic-control interface	1038
35 LOOPBACK DETECTION COMMANDS	1041
loopback-detection	1042
loopback-detection mode	1042
loopback-detection recover-time	1043
loopback-detection transmit-interval	1044
loopback-detection release	1044
show loopback-detection	1044
36 UNIDIRECTIONAL LINK DETECTION COMMANDS	1047
udld message-interval	1047
udld aggressive	1048
udld port	1049
show udld	1050
37 ADDRESS TABLE COMMANDS	1053
mac-address-table aging-time	1053
mac-address-table static	1054
clear mac-address-table dynamic	1055
show mac-address-table	1055
show mac-address-table aging-time	1056
show mac-address-table count	1057
38 SPANNING TREE COMMANDS	1059
spanning-tree	1060

spanning-tree cisco-prestandard	1061
spanning-tree forward-time	1061
spanning-tree hello-time	1062
spanning-tree max-age	1063
spanning-tree mode	1063
spanning-tree pathcost method	1065
spanning-tree priority	1065
spanning-tree mst configuration	1066
spanning-tree system-bpdu-flooding	1067
spanning-tree transmission-limit	1067
max-hops	1068
mst priority	1068
mst vlan	1069
name	1070
revision	1070
spanning-tree bpdu-filter	1071
spanning-tree bpdu-guard	1072
spanning-tree cost	1073
spanning-tree edge-port	1074
spanning-tree link-type	1075
spanning-tree loopback-detection	1075
spanning-tree loopback-detection action	1076
spanning-tree loopback-detection release-mode	1077
spanning-tree loopback-detection trap	1078
spanning-tree mst cost	1078
spanning-tree mst port-priority	1079
spanning-tree port-bpdu-flooding	1080
spanning-tree port-priority	1080
spanning-tree root-guard	1081
spanning-tree spanning-disabled	1082
spanning-tree loopback-detection release	1082
spanning-tree protocol-migration	1083
show spanning-tree	1084
show spanning-tree mst configuration	1086
39 ERPS COMMANDS	1087
erps	1089

erps domain	1089
control-vlan	1090
enable	1091
guard-timer	1092
holdoff-timer	1092
major-domain	1093
meg-level	1094
mep-monitor	1094
node-id	1095
non-erps-dev-protect	1096
non-revertive	1097
propagate-tc	1101
raps-def-mac	1102
raps-without-vc	1102
ring-port	1104
rpl neighbor	1105
rpl owner	1106
version	1107
wtr-timer	1108
clear erps statistics	1108
erps clear	1109
erps forced-switch	1109
erps manual-switch	1111
show erps	1113
40 VLAN COMMANDS	1119
GVRP and Bridge Extension Commands	1120
bridge-ext gvrp	1120
garp timer	1121
switchport forbidden vlan	1122
switchport gvrp	1122
show bridge-ext	1123
show garp timer	1124
show gvrp configuration	1124
Editing VLAN Groups	1125
vlan database	1125
vlan	1126

Configuring VLAN Interfaces	1127
interface vlan	1127
switchport acceptable-frame-types	1128
switchport allowed vlan	1129
switchport ingress-filtering	1130
switchport mode	1131
switchport native vlan	1131
vlan-trunking	1132
Displaying VLAN Information	1134
show vlan	1134
Configuring IEEE 802.1Q Tunneling	1135
dot1q-tunnel system-tunnel-control	1136
switchport dot1q-tunnel mode	1137
switchport dot1q-tunnel service match cvid	1138
switchport dot1q-tunnel tpid	1140
show dot1q-tunnel	1141
Configuring L2CP Tunneling	1142
l2protocol-tunnel tunnel-dmac	1142
switchport l2protocol-tunnel	1144
show l2protocol-tunnel	1145
Configuring VLAN Translation	1146
switchport vlan-translation	1146
show vlan-translation	1147
Configuring Port-based Traffic Segmentation	1148
traffic-segmentation	1148
traffic-segmentation session	1150
traffic-segmentation uplink/downlink	1150
traffic-segmentation uplink-to-uplink	1151
show traffic-segmentation	1152
Configuring Protocol-based VLANs	1152
protocol-vlan protocol-group (Configuring Groups)	1153
protocol-vlan protocol-group (Configuring Interfaces)	1154
show protocol-vlan protocol-group	1155
show interfaces protocol-vlan protocol-group	1156
Configuring IP Subnet VLANs	1156
subnet-vlan	1157

show subnet-vlan	1158
Configuring MAC Based VLANs	1158
mac-vlan	1159
show mac-vlan	1159
Configuring Voice VLANs	1160
voice vlan	1160
voice vlan aging	1161
voice vlan mac-address	1162
switchport voice vlan	1163
switchport voice vlan priority	1163
switchport voice vlan rule	1164
switchport voice vlan security	1165
show voice vlan	1165
41 CLASS OF SERVICE COMMANDS	1167
Priority Commands (Layer 2)	1167
queue mode	1168
queue weight	1169
switchport priority default	1170
show queue mode	1171
show queue weight	1171
Priority Commands (Layer 3 and 4)	1172
qos map cos-dscp	1172
qos map dscp-mutation	1174
qos map phb-queue	1175
qos map trust-mode	1176
show qos map cos-dscp	1177
show qos map dscp-mutation	1177
show qos map phb-queue	1178
show qos map trust-mode	1179
42 QUALITY OF SERVICE COMMANDS	1181
class-map	1182
description	1183
match	1184
rename	1185
policy-map	1186
class	1186

police flow	1188
police srtcm-color	1189
police trtcm-color	1192
set cos	1194
set ip dscp	1195
set phb	1196
service-policy	1197
show class-map	1197
show policy-map	1198
show policy-map interface	1199
43 MULTICAST FILTERING COMMANDS	1201
IGMP Snooping	1201
ip igmp snooping	1203
ip igmp snooping priority	1203
ip igmp snooping proxy-reporting	1204
ip igmp snooping querier	1205
ip igmp snooping router-alert-option-check	1205
ip igmp snooping router-port-expire-time	1206
ip igmp snooping tcn-flood	1206
ip igmp snooping tcn-query-solicit	1208
ip igmp snooping unregistered-data-flood	1208
ip igmp snooping unsolicited-report-interval	1209
ip igmp snooping version	1210
ip igmp snooping version-exclusive	1210
ip igmp snooping vlan general-query-suppression	1211
ip igmp snooping vlan immediate-leave	1212
ip igmp snooping vlan last-memb-query-count	1213
ip igmp snooping vlan last-memb-query-intvl	1213
ip igmp snooping vlan mrd	1214
ip igmp snooping vlan proxy-address	1215
ip igmp snooping vlan query-interval	1216
ip igmp snooping vlan query-resp-intvl	1217
ip igmp snooping vlan static	1218
show ip igmp snooping	1218
show ip igmp snooping group	1220
show ip igmp snooping mrouter	1221

show ip igmp snooping statistics	1221
Static Multicast Routing	1223
ip igmp snooping vlan mrouter	1224
IGMP Filtering and Throttling	1225
ip igmp filter (Global Configuration)	1225
ip igmp profile	1226
permit, deny	1226
range	1227
ip igmp filter (Interface Configuration)	1228
ip igmp max-groups	1228
ip igmp max-groups action	1229
ip igmp query-drop	1230
show ip igmp filter	1230
show ip igmp profile	1231
show ip igmp query-drop	1231
show ip igmp throttle interface	1232
MVR for IPv4	1233
mvr	1234
mvr associated-profile	1234
mvr domain	1235
mvr profile	1235
mvr proxy-query-interval	1236
mvr priority	1237
mvr proxy-switching	1237
mvr robustness-value	1239
mvr source-port-mode dynamic	1239
mvr upstream-source-ip	1240
mvr vlan	1241
mvr immediate-leave	1241
mvr type	1242
mvr vlan group	1243
show mvr	1244
show mvr associated-profile	1245
show mvr interface	1246
show mvr members	1247
show mvr profile	1249

show mvr statistics	1249
MVR for IPv6	1252
mvr6 associated-profile	1253
mvr6 domain	1253
mvr6 profile	1254
mvr6 proxy-query-interval	1255
mvr6 proxy-switching	1255
mvr6 robustness-value	1256
mvr6 source-port-mode dynamic	1257
mvr6 upstream-source-ip	1258
mvr6 vlan	1258
mvr6 immediate-leave	1259
mvr6 type	1260
mvr6 vlan group	1261
show mvr6	1262
show mvr6 associated-profile	1263
show mvr6 interface	1263
show mvr6 members	1264
show mvr6 profile	1265
show mvr6 statistics	1266
44 LLDP COMMANDS	1269
lldp	1271
lldp holdtime-multiplier	1271
lldp med-fast-start-count	1272
lldp notification-interval	1272
lldp refresh-interval	1273
lldp reinit-delay	1273
lldp tx-delay	1274
lldp admin-status	1275
lldp basic-tlv management-ip-address	1275
lldp basic-tlv port-description	1276
lldp basic-tlv system-capabilities	1277
lldp basic-tlv system-description	1277
lldp basic-tlv system-name	1278
lldp dot1-tlv proto-ident	1278
lldp dot1-tlv proto-vid	1279

lldp dot1-tlv pvid	1279
lldp dot1-tlv vlan-name	1280
lldp dot3-tlv link-agg	1280
lldp dot3-tlv mac-phy	1281
lldp dot3-tlv max-frame	1281
lldp dot3-tlv poe	1282
lldp med-location civic-addr	1282
lldp med-notification	1284
lldp med-tlv ext-poe	1285
lldp med-tlv inventory	1285
lldp med-tlv location	1286
lldp med-tlv med-cap	1286
lldp med-tlv network-policy	1287
lldp notification	1287
show lldp config	1288
show lldp info local-device	1289
show lldp info remote-device	1290
show lldp info statistics	1293
45 CFM COMMANDS	1295
Defining CFM Structures	1298
ethernet cfm ais level	1298
ethernet cfm ais ma	1299
ethernet cfm ais period	1300
ethernet cfm ais suppress alarm	1300
ethernet cfm domain	1301
ethernet cfm enable	1303
ma index name	1304
ma index name-format	1305
ethernet cfm mep	1306
ethernet cfm port-enable	1307
clear ethernet cfm ais mpid	1307
show ethernet cfm configuration	1308
show ethernet cfm md	1310
show ethernet cfm ma	1310
show ethernet cfm maintenance-points local	1311
show ethernet cfm maintenance-points local detail mep	1312

show ethernet cfm maintenance-points remote detail	1313
Continuity Check Operations	1315
ethernet cfm cc ma interval	1315
ethernet cfm cc enable	1316
snmp-server enable traps ethernet cfm cc	1317
mep archive-hold-time	1318
clear ethernet cfm maintenance-points remote	1318
clear ethernet cfm errors	1319
show ethernet cfm errors	1320
Cross Check Operations	1321
ethernet cfm mep crosscheck start-delay	1321
snmp-server enable traps ethernet cfm crosscheck	1321
mep crosscheck mpid	1322
ethernet cfm mep crosscheck	1323
show ethernet cfm maintenance-points remote crosscheck	1324
Link Trace Operations	1324
ethernet cfm linktrace cache	1324
ethernet cfm linktrace cache hold-time	1325
ethernet cfm linktrace cache size	1326
ethernet cfm linktrace	1327
clear ethernet cfm linktrace-cache	1328
show ethernet cfm linktrace-cache	1328
Loopback Operations	1329
ethernet cfm loopback	1329
Fault Generator Operations	1330
mep fault-notify alarm-time	1330
mep fault-notify lowest-priority	1331
mep fault-notify reset-time	1333
show ethernet cfm fault-notify-generator	1333
Delay Measure Operations	1334
ethernet cfm delay-measure two-way	1334
46 OAM COMMANDS	1337
efm oam	1338
efm oam critical-link-event	1338
efm oam link-monitor frame	1339
efm oam link-monitor frame threshold	1339

efm oam link-monitor frame window	1340
efm oam mode	1341
clear efm oam counters	1341
efm oam remote-loopback	1342
efm oam remote-loopback test	1343
show efm oam counters interface	1344
show efm oam event-log interface	1344
show efm oam remote-loopback interface	1345
show efm oam status interface	1345
show efm oam status remote interface	1346
47 DOMAIN NAME SERVICE COMMANDS	1347
ip domain-list	1347
ip domain-lookup	1348
ip domain-name	1349
ip host	1350
ip name-server	1351
ipv6 host	1352
clear dns cache	1352
clear host	1353
show dns	1353
show dns cache	1354
show hosts	1354
48 DHCP COMMANDS	1357
DHCP Client	1357
DHCP for IPv4	1358
ip dhcp client class-id	1358
ip dhcp restart client	1359
DHCP for IPv6	1360
ipv6 dhcp client rapid-commit vlan	1360
ipv6 dhcp restart client vlan	1361
show ipv6 dhcp duid	1362
show ipv6 dhcp vlan	1363
ipv6 dhcp client rapid-commit vlan	1363
DHCP Relay	1364
ip dhcp relay server	1364
ip dhcp restart relay	1365

49 IP INTERFACE COMMANDS	1367
IPv4 Interface	1367
Basic IPv4 Configuration	1368
ip address	1368
ip default-gateway	1370
show ip interface	1371
show ip traffic	1371
traceroute	1372
ping	1373
ARP Configuration	1374
arp	1375
arp timeout	1376
ip proxy-arp	1376
clear arp-cache	1377
show arp	1377
IPv6 Interface	1378
Interface Address Configuration and Utilities	1379
ipv6 default-gateway	1379
ipv6 address	1380
ipv6 address autoconfig	1381
ipv6 address eui-64	1383
ipv6 address link-local	1385
ipv6 enable	1386
ipv6 mtu	1387
show ipv6 default-gateway	1388
show ipv6 interface	1388
show ipv6 mtu	1390
show ipv6 traffic	1391
clear ipv6 traffic	1395
ping6	1396
traceroute6	1397
Neighbor Discovery	1398
ipv6 hop-limit	1398
ipv6 nd dad attempts	1399
ipv6 nd ns-interval	1400
ipv6 nd raguard	1401

ipv6 nd reachable-time	1402
clear ipv6 neighbors	1403
show ipv6 nd raguard	1403
show ipv6 neighbors	1404
50 IP ROUTING COMMANDS	1407
Global Routing Configuration	1407
IPv4 Commands	1408
ip route	1408
show ip route	1409
show ip route database	1410
show ip route summary	1410
show ip traffic	1411
Routing Information Protocol (RIP)	1412
router rip	1413
default-information originate	1413
default-metric	1414
distance	1415
maximum-prefix	1416
neighbor	1416
network	1417
passive-interface	1418
redistribute	1418
timers basic	1420
version	1421
ip rip authentication mode	1422
ip rip authentication string	1423
ip rip receive version	1423
ip rip receive-packet	1424
ip rip send version	1425
ip rip send-packet	1426
ip rip split-horizon	1426
clear ip rip route	1427
show ip protocols rip	1428
show ip rip	1428

SECTION IV	APPENDICES	1431
	A SOFTWARE SPECIFICATIONS	1433
	Software Features	1433
	Management Features	1434
	Standards	1435
	Management Information Bases	1435
	B TROUBLESHOOTING	1437
	Problems Accessing the Management Interface	1437
	Using System Logs	1438
	C LICENSE INFORMATION	1439
	The GNU General Public License	1439
	GLOSSARY	1443
	COMMAND LIST	1451
	INDEX	1461

FIGURES

Figure 1: Home Page	100
Figure 2: Front Panel Indicators	101
Figure 3: System Information	120
Figure 4: General Switch Information	122
Figure 5: Configuring Support for Jumbo Frames	123
Figure 6: Displaying Bridge Extension Configuration	124
Figure 7: Copy Firmware	127
Figure 8: Saving the Running Configuration	128
Figure 9: Setting Start-Up Files	129
Figure 10: Displaying System Files	129
Figure 11: Configuring Automatic Code Upgrade	133
Figure 12: Manually Setting the System Clock	135
Figure 13: Setting the Polling Interval for SNTP	136
Figure 14: Configuring NTP	137
Figure 15: Specifying SNTP Time Servers	138
Figure 16: Adding an NTP Time Server	139
Figure 17: Showing the NTP Time Server List	139
Figure 18: Adding an NTP Authentication Key	140
Figure 19: Showing the NTP Authentication Key List	140
Figure 20: Setting the Time Zone	141
Figure 21: Console Port Settings	143
Figure 22: Telnet Connection Settings	145
Figure 23: Displaying CPU Utilization	146
Figure 24: Displaying Memory Utilization	147
Figure 25: Restarting the Switch (Immediately)	149
Figure 26: Restarting the Switch (In)	149
Figure 27: Restarting the Switch (At)	150
Figure 28: Restarting the Switch (Regularly)	150
Figure 29: Configuring Connections by Port List	154
Figure 30: Configuring Connections by Port Range	155
Figure 31: Displaying Port Information	156

Figure 32: Configuring Local Port Mirroring	156
Figure 33: Configuring Local Port Mirroring	157
Figure 34: Displaying Local Port Mirror Sessions	158
Figure 35: Configuring Remote Port Mirroring	158
Figure 36: Configuring Remote Port Mirroring (Source)	161
Figure 37: Configuring Remote Port Mirroring (Intermediate)	162
Figure 38: Configuring Remote Port Mirroring (Destination)	162
Figure 39: Showing Port Statistics (Table)	165
Figure 40: Showing Port Statistics (Chart)	166
Figure 41: Performing Cable Tests	168
Figure 42: Configuring Static Trunks	169
Figure 43: Creating Static Trunks	170
Figure 44: Adding Static Trunks Members	171
Figure 45: Configuring Connection Parameters for a Static Trunk	171
Figure 46: Showing Information for Static Trunks	172
Figure 47: Configuring Dynamic Trunks	172
Figure 48: Configuring the LACP Aggregator Admin Key	175
Figure 49: Enabling LACP on a Port	175
Figure 50: Configuring LACP Parameters on a Port	176
Figure 51: Showing Members of a Dynamic Trunk	176
Figure 52: Configuring Connection Settings for Dynamic Trunks	177
Figure 53: Displaying Connection Parameters for Dynamic Trunks	177
Figure 54: Displaying LACP Port Counters	179
Figure 55: Displaying LACP Port Internal Information	180
Figure 56: Displaying LACP Port Remote Information	182
Figure 57: Enabling Power Savings	184
Figure 58: Enabling Traffic Flow Sampling	185
Figure 59: Configuring Interface Settings for Traffic Flow Sampling	187
Figure 60: Enabling Traffic Segmentation	188
Figure 61: Configuring Members for Traffic Segmentation	190
Figure 62: Showing Traffic Segmentation Members	190
Figure 63: Configuring VLAN Trunking	191
Figure 64: Configuring VLAN Trunking	192
Figure 65: VLAN Compliant and VLAN Non-compliant Devices	194
Figure 66: Using GVRP	196
Figure 67: Creating Static VLANs	198

Figure 68: Modifying Settings for Static VLANs	198
Figure 69: Showing Static VLANs	198
Figure 70: Configuring Static Members by VLAN Index	201
Figure 71: Configuring Static VLAN Members by Interface	202
Figure 72: Configuring Static VLAN Members by Interface Range	203
Figure 73: Configuring Global Status of GVRP	205
Figure 74: Configuring GVRP for an Interface	205
Figure 75: Showing Dynamic VLANs Registered on the Switch	206
Figure 76: Showing the Members of a Dynamic VLAN	206
Figure 77: QinQ Operational Concept	207
Figure 78: Enabling QinQ Tunneling	211
Figure 79: Configuring CVLAN to SPVLAN Mapping Entries	212
Figure 80: Showing CVLAN to SPVLAN Mapping Entries	213
Figure 81: Adding an Interface to a QinQ Tunnel	214
Figure 82: Configuring Protocol VLANs	216
Figure 83: Displaying Protocol VLANs	217
Figure 84: Assigning Interfaces to Protocol VLANs	218
Figure 85: Showing the Interface to Protocol Group Mapping	219
Figure 86: Configuring IP Subnet VLANs	220
Figure 87: Showing IP Subnet VLANs	221
Figure 88: Configuring MAC-Based VLANs	222
Figure 89: Showing MAC-Based VLANs	222
Figure 90: Configuring VLAN Mirroring	224
Figure 91: Showing the VLANs to Mirror	224
Figure 92: Configuring VLAN Translation	225
Figure 93: Configuring VLAN Translation	226
Figure 94: Showing the Entries for VLAN Translation	226
Figure 95: Configuring Static MAC Addresses	228
Figure 96: Displaying Static MAC Addresses	229
Figure 97: Setting the Address Aging Time	229
Figure 98: Displaying the Dynamic MAC Address Table	231
Figure 99: Clearing Entries in the Dynamic MAC Address Table	232
Figure 100: Mirroring Packets Based on the Source MAC Address	233
Figure 101: Showing the Source MAC Addresses to Mirror	233
Figure 102: STP Root Ports and Designated Ports	236
Figure 103: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree	237

Figure 104: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree	237
Figure 105: Configuring Port Loopback Detection	239
Figure 106: Configuring Global Settings for STA (STP)	244
Figure 107: Configuring Global Settings for STA (RSTP)	244
Figure 108: Configuring Global Settings for STA (MSTP)	245
Figure 109: Displaying Global Settings for STA	246
Figure 110: Configuring Interface Settings for STA	250
Figure 111: STA Port Roles	252
Figure 112: Displaying Interface Settings for STA	252
Figure 113: Creating an MST Instance	254
Figure 114: Displaying MST Instances	254
Figure 115: Modifying the Priority for an MST Instance	255
Figure 116: Displaying Global Settings for an MST Instance	255
Figure 117: Adding a VLAN to an MST Instance	256
Figure 118: Displaying Members of an MST Instance	256
Figure 119: Configuring MSTP Interface Settings	258
Figure 120: Displaying MSTP Interface Settings	258
Figure 121: Configuring Rate Limits	260
Figure 122: Configuring Storm Control	262
Figure 123: Storm Control by Limiting the Traffic Rate	263
Figure 124: Storm Control by Shutting Down a Port	264
Figure 125: Configuring ATC Timers	265
Figure 126: Configuring ATC Interface Attributes	268
Figure 127: Setting the Default Port Priority	270
Figure 128: Setting the Queue Mode (Strict)	272
Figure 129: Setting the Queue Mode (WRR)	272
Figure 130: Setting the Queue Mode (Strict and WRR)	273
Figure 131: Mapping CoS Values to Egress Queues	275
Figure 132: Showing CoS Values to Egress Queue Mapping	275
Figure 133: Setting the Trust Mode	277
Figure 134: Configuring DSCP to DSCP Internal Mapping	279
Figure 135: Showing DSCP to DSCP Internal Mapping	279
Figure 136: Configuring CoS to DSCP Internal Mapping	281
Figure 137: Showing CoS to DSCP Internal Mapping	282
Figure 138: Configuring a Class Map	285
Figure 139: Showing Class Maps	286

Figure 140:	Adding Rules to a Class Map	286
Figure 141:	Showing the Rules for a Class Map	287
Figure 142:	Configuring a Policy Map	294
Figure 143:	Showing Policy Maps	295
Figure 144:	Adding Rules to a Policy Map	296
Figure 145:	Showing the Rules for a Policy Map	296
Figure 146:	Attaching a Policy Map to a Port	298
Figure 147:	Configuring a Voice VLAN	301
Figure 148:	Configuring an OUI Telephony List	302
Figure 149:	Showing an OUI Telephony List	302
Figure 150:	Configuring Port Settings for a Voice VLAN	304
Figure 151:	Configuring the Authentication Sequence	308
Figure 152:	Authentication Server Operation	308
Figure 153:	Configuring Remote Authentication Server (RADIUS)	311
Figure 154:	Configuring Remote Authentication Server (TACACS+)	312
Figure 155:	Configuring AAA Server Groups	312
Figure 156:	Showing AAA Server Groups	313
Figure 157:	Configuring Global Settings for AAA Accounting	315
Figure 158:	Configuring AAA Accounting Methods	316
Figure 159:	Showing AAA Accounting Methods	316
Figure 160:	Configuring AAA Accounting Service for 802.1X Service	317
Figure 161:	Configuring AAA Accounting Service for Command Service	317
Figure 162:	Configuring AAA Accounting Service for Exec Service	318
Figure 163:	Displaying a Summary of Applied AAA Accounting Methods	318
Figure 164:	Displaying Statistics for AAA Accounting Sessions	319
Figure 165:	Configuring AAA Authorization Methods	320
Figure 166:	Showing AAA Authorization Methods	321
Figure 167:	Configuring AAA Authorization Methods for Exec Service	321
Figure 168:	Displaying the Applied AAA Authorization Method	321
Figure 169:	Configuring User Accounts	323
Figure 170:	Showing User Accounts	323
Figure 171:	Configuring Global Settings for Web Authentication	325
Figure 172:	Configuring Interface Settings for Web Authentication	326
Figure 173:	Configuring Global Settings for Network Access	330
Figure 174:	Configuring Interface Settings for Network Access	332
Figure 175:	Configuring Link Detection for Network Access	333

Figure 176:	Configuring a MAC Address Filter for Network Access	334
Figure 177:	Showing the MAC Address Filter Table for Network Access	334
Figure 178:	Showing Addresses Authenticated for Network Access	336
Figure 179:	Configuring HTTPS	338
Figure 180:	Downloading the Secure-Site Certificate	339
Figure 181:	Configuring the SSH Server	343
Figure 182:	Generating the SSH Host Key Pair	345
Figure 183:	Showing the SSH Host Key Pair	345
Figure 184:	Copying the SSH User's Public Key	346
Figure 185:	Showing the SSH User's Public Key	347
Figure 186:	Setting the Name of a Time Range	350
Figure 187:	Showing a List of Time Ranges	350
Figure 188:	Add a Rule to a Time Range	351
Figure 189:	Showing the Rules Configured for a Time Range	351
Figure 190:	Showing TCAM Utilization	352
Figure 191:	Creating an ACL	353
Figure 192:	Showing a List of ACLs	354
Figure 193:	Configuring a Standard IPv4 ACL	355
Figure 194:	Configuring an Extended IPv4 ACL	358
Figure 195:	Configuring a Standard IPv6 ACL	359
Figure 196:	Configuring an Extended IPv6 ACL	361
Figure 197:	Configuring a MAC ACL	363
Figure 198:	Configuring a ARP ACL	365
Figure 199:	Binding a Port to an ACL	367
Figure 200:	Configuring ACL Mirroring	368
Figure 201:	Showing the VLANs to Mirror	368
Figure 202:	Showing ACL Statistics	370
Figure 203:	Configuring Global Settings for ARP Inspection	373
Figure 204:	Configuring VLAN Settings for ARP Inspection	374
Figure 205:	Configuring Interface Settings for ARP Inspection	376
Figure 206:	Displaying Statistics for ARP Inspection	377
Figure 207:	Displaying the ARP Inspection Log	378
Figure 208:	Creating an IP Address Filter for Management Access	379
Figure 209:	Showing IP Addresses Authorized for Management Access	380
Figure 210:	Configuring Port Security	382
Figure 211:	Configuring Port Security	383

Figure 212:	Configuring Global Settings for 802.1X Port Authentication	385
Figure 213:	Configuring Interface Settings for 802.1X Port Authenticator	389
Figure 214:	Configuring Interface Settings for 802.1X Port Supplicant	391
Figure 215:	Showing Statistics for 802.1X Port Authenticator	393
Figure 216:	Showing Statistics for 802.1X Port Supplicant	394
Figure 217:	Protecting Against DoS Attacks	396
Figure 218:	Setting the Filter Type for IP Source Guard	398
Figure 219:	Configuring Static Bindings for IP Source Guard	400
Figure 220:	Displaying Static Bindings for IP Source Guard	400
Figure 221:	Showing the IP Source Guard Binding Table	402
Figure 222:	Configuring Global Settings for DHCP Snooping	406
Figure 223:	Configuring DHCP Snooping on a VLAN	407
Figure 224:	Configuring the Port Mode for DHCP Snooping	408
Figure 225:	Displaying the Binding Table for DHCP Snooping	409
Figure 226:	Configuring Settings for System Memory Logs	413
Figure 227:	Showing Error Messages Logged to System Memory	414
Figure 228:	Configuring Settings for Remote Logging of Error Messages	415
Figure 229:	Configuring SMTP Alert Messages	416
Figure 230:	Configuring LLDP Timing Attributes	418
Figure 231:	Configuring LLDP Interface Attributes	422
Figure 232:	Configuring the Civic Address for an LLDP Interface	424
Figure 233:	Showing the Civic Address for an LLDP Interface	424
Figure 234:	Displaying Local Device Information for LLDP (General)	427
Figure 235:	Displaying Local Device Information for LLDP (Port)	427
Figure 236:	Displaying Local Device Information for LLDP (Port Details)	428
Figure 237:	Displaying Remote Device Information for LLDP (Port)	434
Figure 238:	Displaying Remote Device Information for LLDP (Port Details)	435
Figure 239:	Displaying Remote Device Information for LLDP (End Node)	436
Figure 240:	Displaying LLDP Device Statistics (General)	438
Figure 241:	Displaying LLDP Device Statistics (Port)	438
Figure 242:	Showing the Switch's PoE Budget (ECS4510-28P)	440
Figure 243:	Setting a Port's PoE Budget	442
Figure 244:	Configuring Global Settings for SNMP	445
Figure 245:	Configuring the Local Engine ID for SNMP	446
Figure 246:	Configuring a Remote Engine ID for SNMP	447
Figure 247:	Showing Remote Engine IDs for SNMP	448

Figure 248: Creating an SNMP View	449
Figure 249: Showing SNMP Views	449
Figure 250: Adding an OID Subtree to an SNMP View	450
Figure 251: Showing the OID Subtree Configured for SNMP Views	450
Figure 252: Creating an SNMP Group	455
Figure 253: Showing SNMP Groups	455
Figure 254: Setting Community Access Strings	456
Figure 255: Showing Community Access Strings	457
Figure 256: Configuring Local SNMPv3 Users	458
Figure 257: Showing Local SNMPv3 Users	459
Figure 258: Configuring Remote SNMPv3 Users	461
Figure 259: Showing Remote SNMPv3 Users	461
Figure 260: Configuring Trap Managers (SNMPv1)	465
Figure 261: Configuring Trap Managers (SNMPv2c)	465
Figure 262: Configuring Trap Managers (SNMPv3)	466
Figure 263: Showing Trap Managers	466
Figure 264: Creating SNMP Notification Logs	468
Figure 265: Showing SNMP Notification Logs	468
Figure 266: Showing SNMP Statistics	470
Figure 267: Configuring an RMON Alarm	472
Figure 268: Showing Configured RMON Alarms	473
Figure 269: Configuring an RMON Event	475
Figure 270: Showing Configured RMON Events	475
Figure 271: Configuring an RMON History Sample	477
Figure 272: Showing Configured RMON History Samples	477
Figure 273: Showing Collected RMON History Samples	478
Figure 274: Configuring an RMON Statistical Sample	479
Figure 275: Showing Configured RMON Statistical Samples	480
Figure 276: Showing Collected RMON Statistical Samples	480
Figure 277: Configuring a Switch Cluster	482
Figure 278: Configuring a Cluster Members	483
Figure 279: Showing Cluster Members	484
Figure 280: Showing Cluster Candidates	484
Figure 281: Managing a Cluster Member	485
Figure 282: ERPS Ring Components	486
Figure 283: Ring Interconnection Architecture (Multi-ring/Ladder Network)	488

Figure 284:	Setting ERPS Global Status	490
Figure 285:	Sub-ring with Virtual Channel	499
Figure 286:	Sub-ring without Virtual Channel	500
Figure 287:	Creating an ERPS Ring	504
Figure 288:	Creating an ERPS Ring	505
Figure 289:	Showing Configured ERPS Rings	505
Figure 290:	Blocking an ERPS Ring Port	510
Figure 291:	Single CFM Maintenance Domain	511
Figure 292:	Multiple CFM Maintenance Domains	512
Figure 293:	Configuring Global Settings for CFM	516
Figure 294:	Configuring Interfaces for CFM	517
Figure 295:	Configuring Maintenance Domains	521
Figure 296:	Showing Maintenance Domains	521
Figure 297:	Configuring Detailed Settings for Maintenance Domains	522
Figure 298:	Creating Maintenance Associations	525
Figure 299:	Showing Maintenance Associations	526
Figure 300:	Configuring Detailed Settings for Maintenance Associations	526
Figure 301:	Configuring Maintenance End Points	528
Figure 302:	Showing Maintenance End Points	528
Figure 303:	Configuring Remote Maintenance End Points	530
Figure 304:	Showing Remote Maintenance End Points	530
Figure 305:	Transmitting Link Trace Messages	532
Figure 306:	Transmitting Loopback Messages	533
Figure 307:	Transmitting Delay-Measure Messages	535
Figure 308:	Showing Information on Local MEPs	536
Figure 309:	Showing Detailed Information on Local MEPs	538
Figure 310:	Showing Information on Local MIPs	539
Figure 311:	Showing Information on Remote MEPs	540
Figure 312:	Showing Detailed Information on Remote MEPs	542
Figure 313:	Showing the Link Trace Cache	544
Figure 314:	Showing Settings for the Fault Notification Generator	545
Figure 315:	Showing Continuity Check Errors	546
Figure 316:	Enabling OAM for Local Ports	549
Figure 317:	Displaying Statistics for OAM Messages	550
Figure 318:	Displaying the OAM Event Log	551
Figure 319:	Displaying Status of Remote Interfaces	552

Figure 320:	Running a Remote Loop Back Test	554
Figure 321:	Displaying the Results of Remote Loop Back Testing	555
Figure 322:	Multicast Filtering Concept	557
Figure 323:	Configuring General Settings for IGMP Snooping	563
Figure 324:	Configuring a Static Interface for a Multicast Router	565
Figure 325:	Showing Static Interfaces Attached a Multicast Router	565
Figure 326:	Showing Current Interfaces Attached a Multicast Router	566
Figure 327:	Assigning an Interface to a Multicast Service	567
Figure 328:	Showing Static Interfaces Assigned to a Multicast Service	567
Figure 329:	Configuring IGMP Snooping on a VLAN	572
Figure 330:	Showing Interface Settings for IGMP Snooping	573
Figure 331:	Dropping IGMP Query or Multicast Data Packets	574
Figure 332:	Showing Multicast Groups Learned by IGMP Snooping	575
Figure 333:	Displaying IGMP Snooping Statistics – Query	577
Figure 334:	Displaying IGMP Snooping Statistics – VLAN	578
Figure 335:	Displaying IGMP Snooping Statistics – Port	578
Figure 336:	Enabling IGMP Filtering and Throttling	580
Figure 337:	Creating an IGMP Filtering Profile	581
Figure 338:	Showing the IGMP Filtering Profiles Created	581
Figure 339:	Adding Multicast Groups to an IGMP Filtering Profile	582
Figure 340:	Showing the Groups Assigned to an IGMP Filtering Profile	582
Figure 341:	Configuring IGMP Filtering and Throttling Interface Settings	584
Figure 342:	MVR Concept	584
Figure 343:	Configuring Global Settings for MVR	587
Figure 344:	Configuring Domain Settings for MVR	588
Figure 345:	Configuring an MVR Group Address Profile	590
Figure 346:	Displaying MVR Group Address Profiles	590
Figure 347:	Assigning an MVR Group Address Profile to a Domain	591
Figure 348:	Showing the MVR Group Address Profiles Assigned to a Domain	591
Figure 349:	Configuring Interface Settings for MVR	594
Figure 350:	Assigning Static MVR Groups to a Port	595
Figure 351:	Showing the Static MVR Groups Assigned to a Port	596
Figure 352:	Displaying MVR Receiver Groups	597
Figure 353:	Displaying MVR Statistics – Query	599
Figure 354:	Displaying MVR Statistics – VLAN	600
Figure 355:	Displaying MVR Statistics – Port	601

Figure 356:	Configuring Global Settings for MVR6	603
Figure 357:	Configuring Domain Settings for MVR6	605
Figure 358:	Configuring an MVR6 Group Address Profile	606
Figure 359:	Displaying MVR6 Group Address Profiles	607
Figure 360:	Assigning an MVR6 Group Address Profile to a Domain	607
Figure 361:	Showing MVR6 Group Address Profiles Assigned to a Domain	608
Figure 362:	Configuring Interface Settings for MVR6	610
Figure 363:	Assigning Static MVR6 Groups to a Port	611
Figure 364:	Showing the Static MVR6 Groups Assigned to a Port	611
Figure 365:	Displaying MVR6 Receiver Groups	612
Figure 366:	Displaying MVR6 Statistics – Query	614
Figure 367:	Displaying MVR6 Statistics – VLAN	615
Figure 368:	Displaying MVR6 Statistics – Port	616
Figure 369:	Configuring a Static IPv4 Address	619
Figure 370:	Configuring a Dynamic IPv4 Address	620
Figure 371:	Showing the Configured IP Address for an Interface	621
Figure 372:	Configuring the IPv6 Default Gateway	622
Figure 373:	Configuring General Settings for an IPv6 Interface	626
Figure 374:	Configuring RA Guard for an IPv6 Interface	627
Figure 375:	Configuring an IPv6 Address	630
Figure 376:	Showing Configured IPv6 Addresses	631
Figure 377:	Showing IPv6 Neighbors	632
Figure 378:	Showing IPv6 Statistics (IPv6)	637
Figure 379:	Showing IPv6 Statistics (ICMPv6)	637
Figure 380:	Showing IPv6 Statistics (UDP)	638
Figure 381:	Showing Reported MTU Values	638
Figure 382:	Configuring General Settings for DNS	640
Figure 383:	Configuring a List of Domain Names for DNS	641
Figure 384:	Showing the List of Domain Names for DNS	641
Figure 385:	Configuring a List of Name Servers for DNS	642
Figure 386:	Showing the List of Name Servers for DNS	643
Figure 387:	Configuring Static Entries in the DNS Table	644
Figure 388:	Showing Static Entries in the DNS Table	644
Figure 389:	Showing Entries in the DNS Cache	645
Figure 390:	Specifying A DHCP Client Identifier	647
Figure 391:	Layer 3 DHCP Relay Service	647

Figure 392: Configuring DHCP Relay Service	648
Figure 393: Configuring Global Settings for PPPoE Intermediate Agent	650
Figure 394: Configuring Interface Settings for PPPoE Intermediate Agent	651
Figure 395: Showing PPPoE Intermediate Agent Statistics	653
Figure 396: Virtual Interfaces and Layer 3 Routing	656
Figure 397: Pinging a Network Device	660
Figure 398: Tracing the Route to a Network Device	661
Figure 399: Proxy ARP	663
Figure 400: Configuring General Settings for ARP	664
Figure 401: Configuring Static ARP Entries	665
Figure 402: Displaying Static ARP Entries	665
Figure 403: Displaying Dynamic ARP Entries	666
Figure 404: Displaying Local ARP Entries	666
Figure 405: Displaying ARP Statistics	667
Figure 406: Configuring Static Routes	668
Figure 407: Displaying Static Routes	669
Figure 408: Displaying the Routing Table	670
Figure 409: Configuring RIP	672
Figure 410: Configuring General Settings for RIP	676
Figure 411: Clearing Entries from the Routing Table	677
Figure 412: Adding Network Interfaces to RIP	678
Figure 413: Showing Network Interfaces Using RIP	679
Figure 414: Specifying a Passive RIP Interface	680
Figure 415: Showing Passive RIP Interfaces	680
Figure 416: Specifying a Static RIP Neighbor	681
Figure 417: Showing Static RIP Neighbors	681
Figure 418: Redistributing External Routes into RIP	682
Figure 419: Showing External Routes Redistributed into RIP	683
Figure 420: Setting the Distance Assigned to External Routes	684
Figure 421: Showing the Distance Assigned to External Routes	684
Figure 422: Configuring a Network Interface for RIP	688
Figure 423: Showing RIP Network Interface Settings	688
Figure 424: Showing RIP Interface Settings	689
Figure 425: Showing RIP Peer Information	690
Figure 426: Resetting RIP Statistics	690
Figure 427: Storm Control by Limiting the Traffic Rate	1026

Figure 428: Storm Control by Shutting Down a Port	1027
Figure 429: Sub-ring with Virtual Channel	1103
Figure 430: Sub-ring without Virtual Channel	1104
Figure 431: Configuring VLAN Trunking	1133
Figure 432: Mapping QinQ Service VLAN to Customer VLAN	1139
Figure 433: Configuring VLAN Translation	1147

TABLES

Table 1: Key Features	69
Table 2: System Defaults	76
Table 3: Options 60, 66 and 67 Statements	91
Table 4: Options 55 and 124 Statements	91
Table 5: Web Page Configuration Buttons	101
Table 6: Switch Main Menu	102
Table 7: Port Statistics	163
Table 8: LACP Port Counters	178
Table 9: LACP Internal Configuration Information	179
Table 10: LACP Remote Device Configuration Information	181
Table 11: Traffic Segmentation Forwarding	189
Table 12: Recommended STA Path Cost Range	247
Table 13: Default STA Path Costs	248
Table 14: IEEE 802.1p Egress Queue Priority Mapping	273
Table 15: CoS Priority Levels	273
Table 16: Mapping Internal Per-hop Behavior to Hardware Queues	274
Table 17: Default Mapping of DSCP Values to Internal PHB/Drop Values	278
Table 18: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	281
Table 19: Dynamic QoS Profiles	327
Table 20: HTTPS System Support	337
Table 21: ARP Inspection Statistics	376
Table 22: ARP Inspection Log	377
Table 23: 802.1X Statistics	391
Table 24: Logging Levels	412
Table 25: LLDP MED Location CA Types	423
Table 26: Chassis ID Subtype	425
Table 27: System Capabilities	425
Table 28: Port ID Subtype	426
Table 29: Remote Port Auto-Negotiation Advertised Capability	430
Table 30: SNMPv3 Security Models and Levels	443
Table 31: Supported Notification Messages	452

Table 32: ERPS Request/State Priority	507
Table 33: Remote MEP Priority Levels	519
Table 34: MEP Defect Descriptions	519
Table 35: OAM Operation State	547
Table 36: Remote Loopback Status	553
Table 37: ShowIPv6 Neighbors - display description	631
Table 38: Show IPv6 Statistics - display description	633
Table 39: Show MTU - display description	638
Table 40: Options 60, 66 and 67 Statements	646
Table 41: Options 55 and 124 Statements	646
Table 42: Address Resolution Protocol	662
Table 43: ARP Statistics	667
Table 44: General Command Modes	699
Table 45: Configuration Command Modes	701
Table 46: Keystroke Commands	702
Table 47: Command Group Index	703
Table 48: General Commands	707
Table 49: System Management Commands	715
Table 50: Device Designation Commands	715
Table 51: Banner Commands	716
Table 52: System Status Commands	725
Table 53: Frame Size Commands	733
Table 54: Flash/File Commands	734
Table 55: File Directory Information	740
Table 56: Line Commands	746
Table 57: Event Logging Commands	757
Table 58: Logging Levels	758
Table 59: show logging flash/ram - display description	762
Table 60: show logging trap - display description	763
Table 61: Event Logging Commands	763
Table 62: Time Commands	767
Table 63: Time Range Commands	776
Table 64: Switch Cluster Commands	779
Table 65: SNMP Commands	785
Table 66: show snmp engine-id - display description	798
Table 67: show snmp group - display description	799

Table 68: show snmp user - display description	800
Table 69: show snmp view - display description	801
Table 70: RMON Commands	807
Table 71: sFlow Commands	815
Table 72: Authentication Commands	823
Table 73: User Access Commands	824
Table 74: Default Login Settings	825
Table 75: Authentication Sequence Commands	827
Table 76: RADIUS Client Commands	830
Table 77: TACACS+ Client Commands	834
Table 78: AAA Commands	838
Table 79: Web Server Commands	847
Table 80: HTTPS System Support	850
Table 81: Telnet Server Commands	850
Table 82: Secure Shell Commands	852
Table 83: show ssh - display description	862
Table 84: 802.1X Port Authentication Commands	862
Table 85: Management IP Filter Commands	877
Table 86: PPPoE Intermediate Agent Commands	879
Table 87: show pppoe intermediate-agent statistics - display description	885
Table 88: General Security Commands	887
Table 89: Management IP Filter Commands	888
Table 90: show port security - display description	890
Table 91: Network Access Commands	892
Table 92: Dynamic QoS Profiles	895
Table 93: Web Authentication	906
Table 94: DHCP Snooping Commands	911
Table 95: Option 82 information	918
Table 96: DHCP Snooping Commands	922
Table 97: IP Source Guard Commands	929
Table 98: ARP Inspection Commands	934
Table 99: DoS Protection Commands	943
Table 100: Access Control List Commands	949
Table 101: IPv4 ACL Commands	949
Table 102: IPv6 ACL Commands	956
Table 103: MAC ACL Commands	962

Table 104:	ARP ACL Commands	967
Table 105:	ACL Information Commands	969
Table 106:	Interface Commands	973
Table 107:	show interfaces switchport - display description	986
Table 108:	Link Aggregation Commands	993
Table 109:	show lacp counters - display description	1003
Table 110:	show lacp internal - display description	1003
Table 111:	show lacp neighbors - display description	1004
Table 112:	show lacp sysid - display description	1005
Table 113:	PoE Commands	1007
Table 114:	show power inline status - display description	1010
Table 115:	show power mainpower - display description	1011
Table 116:	Port Mirroring Commands	1013
Table 117:	Mirror Port Commands	1013
Table 118:	RSPAN Commands	1016
Table 119:	Rate Limit Commands	1023
Table 120:	ATC Commands	1025
Table 121:	Loopback Detection Commands	1041
Table 122:	UniDirectional Link Detection Commands	1047
Table 123:	show udd - display description	1050
Table 124:	Address Table Commands	1053
Table 125:	Spanning Tree Commands	1059
Table 126:	Recommended STA Path Cost Range	1073
Table 127:	Default STA Path Costs	1073
Table 128:	ERPS Commands	1087
Table 129:	ERPS Request/State Priority	1110
Table 130:	show erps - summary display description	1114
Table 131:	show erps domain - detailed display description	1115
Table 132:	show erps statistics - detailed display description	1116
Table 133:	VLAN Commands	1119
Table 134:	GVRP and Bridge Extension Commands	1120
Table 135:	Commands for Editing VLAN Groups	1125
Table 136:	Commands for Configuring VLAN Interfaces	1127
Table 137:	Commands for Displaying VLAN Information	1134
Table 138:	802.1Q Tunneling Commands	1135
Table 139:	L2 Protocol Tunnel Commands	1142

Table 140: VLAN Translation Commands	1146
Table 141: Commands for Configuring Traffic Segmentation	1148
Table 142: Traffic Segmentation Forwarding	1149
Table 143: Protocol-based VLAN Commands	1153
Table 144: IP Subnet VLAN Commands	1156
Table 145: MAC Based VLAN Commands	1158
Table 146: Voice VLAN Commands	1160
Table 147: Priority Commands	1167
Table 148: Priority Commands (Layer 2)	1167
Table 149: Priority Commands (Layer 3 and 4)	1172
Table 150: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	1173
Table 151: Default Mapping of DSCP Values to Internal PHB/Drop Values	1174
Table 152: Mapping Internal Per-hop Behavior to Hardware Queues	1175
Table 153: Quality of Service Commands	1181
Table 154: Multicast Filtering Commands	1201
Table 155: IGMP Snooping Commands	1201
Table 156: show ip igmp snooping statistics input - display description	1222
Table 157: show ip igmp snooping statistics output - display description	1222
Table 158: show ip igmp snooping statistics vlan query - display description	1223
Table 159: Static Multicast Interface Commands	1223
Table 160: IGMP Filtering and Throttling Commands	1225
Table 161: Multicast VLAN Registration for IPv4 Commands	1233
Table 162: show mvr - display description	1245
Table 163: show mvr interface - display description	1246
Table 164: show mvr members - display description	1248
Table 165: show mvr statistics input - display description	1250
Table 166: show mvr statistics output - display description	1250
Table 167: show mvr statistics query - display description	1251
Table 168: Multicast VLAN Registration for IPv6 Commands	1252
Table 169: show mvr6 - display description	1262
Table 170: show mvr6 interface - display description	1264
Table 171: show mvr6 members - display description	1265
Table 172: show mvr6 statistics input - display description	1267
Table 173: show mvr6 statistics output - display description	1267
Table 174: LLDP Commands	1269
Table 175: LLDP MED Location CA Types	1283

Table 176: CFM Commands	1295
Table 177: show ethernet cfm configuration traps - display description	1309
Table 178: show ethernet cfm maintenance-points local detail mep - display	1313
Table 179: show ethernet cfm maintenance-points remote detail - display	1314
Table 180: show ethernet cfm errors - display description	1320
Table 181: show ethernet cfm linktrace-cache - display description	1328
Table 182: Remote MEP Priority Levels	1332
Table 183: MEP Defect Descriptions	1332
Table 184: show fault-notify-generator - display description	1334
Table 185: OAM Commands	1337
Table 186: Address Table Commands	1347
Table 187: show dns cache - display description	1354
Table 188: show hosts - display description	1355
Table 189: DHCP Commands	1357
Table 190: DHCP Client Commands	1357
Table 191: Options 60, 66 and 67 Statements	1358
Table 192: Options 55 and 124 Statements	1359
Table 193: DHCP Relay Option 82 Commands	1364
Table 194: IP Interface Commands	1367
Table 195: IPv4 Interface Commands	1367
Table 196: Basic IP Configuration Commands	1368
Table 197: Address Resolution Protocol Commands	1374
Table 198: IPv6 Configuration Commands	1378
Table 199: show ipv6 interface - display description	1389
Table 200: show ipv6 mtu - display description	1391
Table 201: show ipv6 traffic - display description	1392
Table 202: show ipv6 neighbors - display description	1404
Table 1: IP Routing Commands	1407
Table 2: Global Routing Configuration Commands	1407
Table 3: Routing Information Protocol Commands	1412
Table 4: Troubleshooting Chart	1437

SECTION I

GETTING STARTED

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- ◆ ["Introduction" on page 69](#)
- ◆ ["Initial Switch Configuration" on page 79](#)

This switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

KEY FEATURES

Table 1: Key Features

Feature	Description
Configuration Backup and Restore	Using management station or FTP/TFTP server
Authentication	Console, Telnet, web – user name/password, RADIUS, TACACS+ Port – IEEE 802.1X, MAC address filtering SNMP v1/2c – Community strings SNMP version 3 – MD5 or SHA password Telnet – SSH Web – HTTPS
General Security Measures	AAA ARP Inspection DHCP Snooping (with Option 82 relay information) DoS Protection IP Source Guard PPPoE Intermediate Agent Port Authentication – IEEE 802.1X Port Security – MAC address filtering
Access Control Lists	Supports up to 512 ACLs, 2048 rules per ACL, and 2048 rules per system
DHCP/DHCPv6	Client, Relay, Relay Option 82
DNS	Client and Proxy service
Port Configuration	Speed, duplex mode, and flow control
Port Trunking	Supports up to 16 trunks – static or dynamic trunking (LACP)
Port Mirroring	27 sessions, one or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms
Address Table	16K MAC addresses in the forwarding table, 1K static MAC addresses; 4K IPv4 entries in the host table; 1792 entries in the ARP cache, 256 static ARP entries; 1K IPv4 entries in routing table, 256 static IP routes, 32 IP interfaces; 4K L2 multicast groups

Table 1: Key Features (Continued)

Feature	Description
IP Version 4 and 6	Supports IPv4 and IPv6 addressing and management
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 4093 using IEEE 802.1Q, port-based, protocol-based, voice VLANs, and QinQ tunnel
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP)
Qualify of Service	Supports Differentiated Services (DiffServ)
Link Layer Discovery Protocol	Used to discover basic information about neighboring devices
IP Routing	Routing Information Protocol (RIP), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, and IGMP for Layer 3, and Multicast VLAN Registration
Switch Clustering	Supports up to 36 member switches in a cluster
Connectivity Fault Management	Connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections (IEEE 802.1ag)
ERPS	Supports Ethernet Ring Protection Switching for increased availability of Ethernet rings (G.8032)
Remote Device Management	Supports Ethernet OAM functions for attached CPEs (IEEE 802.3ah, ITU-T Y.1731)

DESCRIPTION OF SOFTWARE FEATURES

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications.

Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

You can save the current configuration settings to a file on the management station (using the web interface) or an FTP/TFTP server (using the web or console interface), and later download this file to restore the switch configuration settings.

AUTHENTICATION This switch authenticates management access via the console port, Telnet, or a web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication server to verify the client's right to access the network via an authentication server (i.e., RADIUS or TACACS+ server).

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/Telnet/web management access. MAC address filtering and IP source guard also provide authenticated port access. While DHCP snooping is provided to prevent malicious attacks from insecure ports. While PPPoE Intermediate Agent supports authentication of a client for a service provider.

ACCESS CONTROL LISTS ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

DHCP DHCP Relay is supported to allow dynamic configuration of local clients from a DHCP server located in a different network. And DHCP Relay Option 82 controls the processing of Option 82 information in DHCP request packets relayed by this device.

PORT CONFIGURATION You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

RATE LIMITING This feature controls 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.

PORT MIRRORING The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

PORT TRUNKING Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 16 trunks.

STORM CONTROL Broadcast, multicast and unknown unicast storm suppression prevents traffic from overwhelming the network. When enabled on a port, the level of traffic passing through the port is restricted. If traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

STATIC MAC ADDRESSES A static address can be assigned to a specific interface on this switch. 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. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IP ADDRESS FILTERING Access to insecure ports can be controlled using DHCP Snooping which filters ingress traffic based on static IP addresses and addresses stored in the DHCP Snooping table. Traffic can also be restricted to specific source IP addresses or source IP/MAC address pairs based on static entries or entries stored in the DHCP Snooping table.

IEEE 802.1D BRIDGE The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

STORE-AND-FORWARD SWITCHING The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 12 Mbits for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

SPANNING TREE ALGORITHM The switch supports these spanning tree protocols:

- ◆ Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others

to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

- ◆ **Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)** – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.
- ◆ **Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s)** – This protocol is a direct extension of RSTP. It 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 (as sometimes occurs with IEEE 802.1D STP).

CONNECTIVITY FAULT MANAGEMENT

The switch provides connectivity fault monitoring for end-to-end connections within a designated service area by using continuity check messages which can detect faults in maintenance points, fault verification through loop back messages, and fault isolation with link trace messages.

VIRTUAL LANS

The switch supports up to 4093 VLANs. 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. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- ◆ Eliminate broadcast storms which severely degrade performance in a flat network.
- ◆ Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- ◆ Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- ◆ Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- ◆ Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

IEEE 802.1Q TUNNELING (QINQ) This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

TRAFFIC PRIORITIZATION This switch prioritizes each packet based on the required level of service, using eight priority queues with strict priority, Weighted Round Robin (WRR), or a combination of strict and weighted queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet using DSCP, or IP Precedence. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

QUALITY OF SERVICE Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

ETHERNET RING PROTECTION SWITCHING ERPS can be used to increase the availability and robustness of Ethernet rings, such as those used in Metropolitan Area Networks (MAN). ERPS provides Layer 2 loop avoidance and fast reconvergence in Layer 2 ring topologies, supporting up to 255 nodes in the ring structure. It can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist within the Ethernet ring.

IP ROUTING The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with static routing, and Routing Information Protocol (RIP).

Static Routing – Traffic is automatically routed between any IP interfaces configured on the switch. Routing to statically configured hosts or subnet addresses is provided based on next-hop entries specified in the static routing table.

RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.

**ADDRESS RESOLUTION
PROTOCOL**

The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (hardware) addresses. This switch supports conventional ARP, which locates 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. Either static or dynamic entries can be configured in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.

MULTICAST FILTERING

Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration. It also supports Multicast VLAN Registration (MVR for IPv4 and MVR6 for IPv6) which allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, while preserving security and data isolation for normal traffic.

**LINK LAYER
DISCOVERY PROTOCOL**

LLDP is used to discover basic information about neighboring devices within the local broadcast domain. LLDP is a Layer 2 protocol that advertises information about the sending device and collects information gathered from neighboring network nodes it discovers.

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. 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. The LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

SYSTEM DEFAULTS

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file.

The following table lists some of the basic system defaults.

Table 2: System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	115200 bps
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	600 seconds
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS+ Authentication	Disabled
	802.1X Port Authentication	Disabled
	MAC Authentication	Disabled
	PPPoE Intermediate Agent	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
	DHCP Snooping	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)

Table 2: System Defaults (Continued)

Function	Parameter	Default
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Enabled (64 kbits/sec)
		Multicast: Disabled Unknown Unicast: Disabled
OAM	Status	Disabled
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Disabled
ERPS	Status	Disabled
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
	QinQ Tunneling	Disabled
	Traffic Prioritization	Ingress Port Priority
		Queue Mode
		Queue Weight
Traffic Prioritization	Class of Service	Enabled
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
IP Settings	Management. VLAN	VLAN 1
	IP Address	DHCP assigned
	Subnet Mask	255.255.255.0
	Default Gateway	Not configured
	DHCP	Client: Enabled
	DNS	Proxy service: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	Multicast VLAN Registration	Disabled
	IGMP Proxy Reporting	Disabled
System Log	Status	Enabled
	Messages Logged to RAM	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled
Switch Clustering	Status	Disabled
	Commander	Disabled

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 83](#).

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 6.x or above, and Mozilla Firefox 3.6.2/4/5. 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 4093 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/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 16)
- ◆ Enable port mirroring
- ◆ Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- ◆ Display system information and statistics

REQUIRED CONNECTIONS

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-232 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.



NOTE: Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see ["Using the Command Line Interface" on page 693](#). For a list of all the CLI commands and detailed information on using the CLI, refer to ["CLI Command Groups" on page 703](#).

REMOTE CONNECTIONS

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, or DHCP protocol.

An IPv4 address for this 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 83](#).



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

NOTE: Any VLAN group can be assigned an IP interface address ([page 83](#)) for managing the switch.

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 from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 6.x or above, or Mozilla Firefox 3.6.2/4/5), or from a network computer using SNMP network management software.

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.

BASIC CONFIGURATION

CONSOLE CONNECTION 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 Username 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 ECS4510-28T* 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 ECS4510-28T/52T Gigabit Ethernet switches, the ECS4510-28F Gigabit Ethernet Fiber Switch, and the ECS4510-28P/52P Gigabit Ethernet PoE switches. Other than the difference in port types, and support for PoE (ECS4510-28P/52P), there are no other significant differences. Therefore nearly all of the screen display examples are based on the ECS4510-28T.

SETTING AN IP ADDRESS

You must establish IP address information for the 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.
- ◆ **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 88](#).

DHCP for IPv6 can be used to acquire stateful address configuration information depending on the advertisements received from other routers, and subsequently from a DHCPv6 server. (For more information, see the description for the "Restart DHCPv6" parameter under ["Configuring IPv6 Interface Settings" on page 622](#).)

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 IPv4 address for VLAN 1 is obtained via DHCP by default.

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 ["Setting the Switch's IP Address \(IP Version 6\)" on page 621](#).

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 up
IPv6 is enabled.
Link-local address:
    fe80::200:e8ff:fe94:4000%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:ff94:4000
    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 00-12-CF-DA-FC-E8
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
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::200:e8ff:fe94:4000%2/64
Global unicast address(es):
  2001:db8:2222:7273::/64, subnet is 2001:db8:2222:7273::/64
Joined group address(es):
  ff02::1:ff94:4000
  ff02::1:ff00:0
  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 — To generate an IPv6 address that can be used in a network containing more than one subnet, the switch can be configured to automatically generate a unique host address based on the local subnet address prefix received in router advertisement messages, and subsequently from a DHCPv6 server. (For more information, see the description for the "Restart DHCPv6" parameter under ["Configuring IPv6 Interface Settings" on page 622.](#))

To dynamically generate an IPv6 host 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 autoconfig" and press <Enter>.
3. Type "ipv6 enable" and press <Enter> to enable IPv6 on an interface that has not been configured with an explicit IPv6 address.

```

Console(config)#interface vlan 1
Console(config-if)#ipv6 address autoconfig
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):
    2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64[AUTOCONFIG]
    valid lifetime 2591978 preferred lifetime 604778
Joined group address(es):
    ff02::1:ff11:6700
    ff02::1:ff00:0
    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#

```

If the DHCP is configured to assign a stateful address, the following type of address settings will be assigned to the specified interface.

```

Console#ipv6 restart client vlan 1
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::2e0:cff:fe01:fd%1/64

```

```
Global unicast address(es):
  2000::74ef:2ff1:c00d:611b/64, subnet is 2000::/64[AUTOCONFIG]
    valid lifetime -1 preferred lifetime -1
  3fff::2e0:cff:fe01:fd/64, subnet is 3fff::/64[AUTOCONFIG]
    valid lifetime 2591819 preferred lifetime 604619
  3fff:1::2e0:cff:fe01:fd/64, subnet is 3fff:1::/64[AUTOCONFIG]
    valid lifetime 2591819 preferred lifetime 604619
Joined group address(es):
ff02::1:ff0d:611b
ff02::1:ff01:fd
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#
```

DOWNLOADING A CONFIGURATION FILE REFERENCED BY 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. 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:

- ◆ 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 3: 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" 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 4: 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 following configuration examples are 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 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" {                      #DHCP Option 60 Vendor class
match if option vendor-class-identifier = "ecs4510-series.cfg";
option tftp-server-name "192.168.255.101";
option bootfile-name "test";
}
```



NOTE: Use "ecs4510-series.cfg" for the vendor-class-identifier in the dhcpd.conf file.

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 ["Setting SNMPv3 Views" on page 448](#)).

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 ["snmp-server host" on page 791](#). 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 ["Simple Network Management Protocol" on page 442](#), or refer to the specific CLI commands for SNMP starting on [page 785](#).

MANAGING SYSTEM FILES

The switch's flash memory supports three types of system files that can be managed by the CLI program, 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/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 95](#) 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. See ["Managing System Files" on page 125](#) for more information.
- ◆ **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

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.

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 file 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#
```

SECTION II

WEB CONFIGURATION

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser.

This section includes these chapters:

- ◆ ["Using the Web Interface" on page 99](#)
- ◆ ["Basic Management Tasks" on page 119](#)
- ◆ ["Interface Configuration" on page 151](#)
- ◆ ["VLAN Configuration" on page 193](#)
- ◆ ["Address Table Settings" on page 227](#)
- ◆ ["Spanning Tree Algorithm" on page 235](#)
- ◆ ["Rate Limit Configuration" on page 227](#)
- ◆ ["Storm Control Configuration" on page 229](#)
- ◆ ["Class of Service" on page 269](#)
- ◆ ["Quality of Service" on page 283](#)
- ◆ ["VoIP Traffic Configuration" on page 299](#)
- ◆ ["Security Measures" on page 305](#)
- ◆ ["Basic Administration Protocols" on page 411](#)
- ◆ ["Multicast Filtering" on page 557](#)
- ◆ ["IP Configuration" on page 617](#)
- ◆ ["IP Services" on page 639](#)
- ◆ ["General IP Routing" on page 655](#)
- ◆ ["Unicast Routing" on page 671](#)

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 6.x or above, or Mozilla Firefox 3.6.2/4/5).



NOTE: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to ["Using the Command Line Interface" on page 693](#).

CONNECTING TO THE WEB INTERFACE

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See ["Setting an IP Address" on page 83](#).)
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See ["Setting Passwords" on page 82](#).)
3. After you enter a user name and password, you will have access to the system configuration program.



NOTE: You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

NOTE: If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

NOTE: If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See ["Configuring Interface Settings for STA" on page 246](#).

NOTE: Users are automatically logged off of the HTTP server or HTTPS server if no input is detected for 600 seconds.

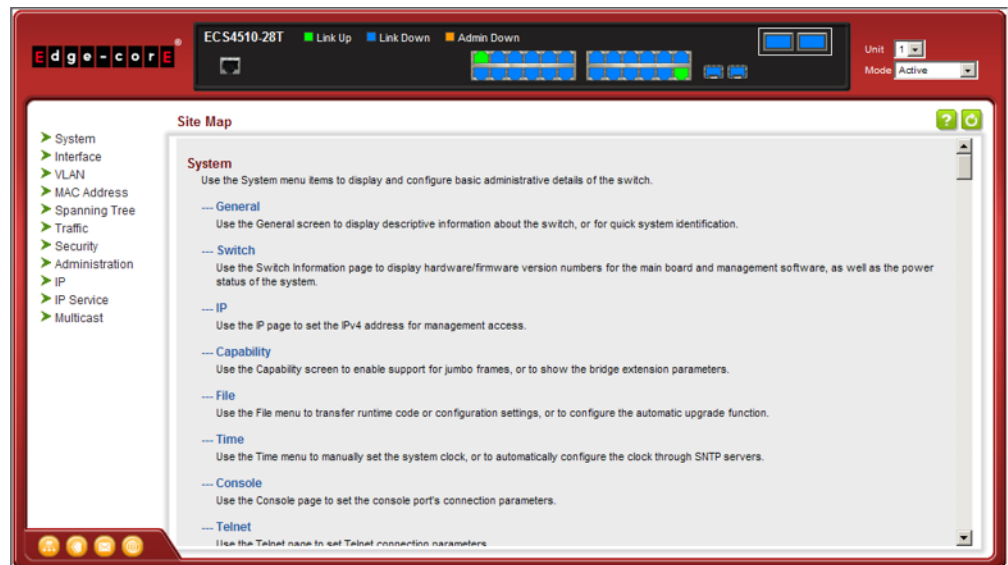
NOTE: Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

NAVIGATING THE WEB BROWSER INTERFACE

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

HOME PAGE When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Home Page









NOTE: This manual covers the ECS4510-28T/52T Gigabit Ethernet switches, the ECS4510-28F Gigabit Ethernet Fiber Switch, and the ECS4510-28P/52P Gigabit Ethernet PoE switches. Other than the difference in port types, and support for PoE (ECS4510-28P/52P), there are no other significant differences. Therefore nearly all of the screen display examples are based on the ECS4610-26T. The panel graphics for both switch types are shown on the following page.

NOTE: You can open a connection to the vendor's web site by clicking on the Edge-core logo.

CONFIGURATION OPTIONS Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

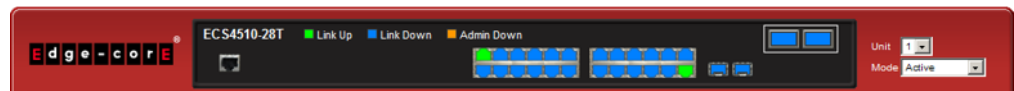
Table 5: Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
	Displays help for the selected page.
	Refreshes the current page.
	Displays the site map.
	Logs out of the management interface.
	Sends mail to the vendor.
	Links to the vendor's web site.

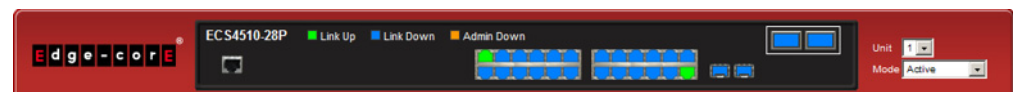
PANEL DISPLAY The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control).

Figure 2: Front Panel Indicators

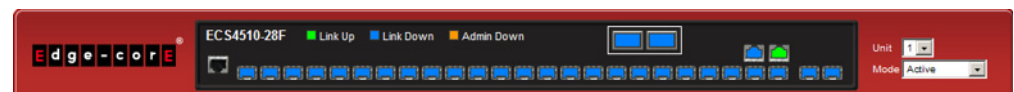
ECS4510-28T



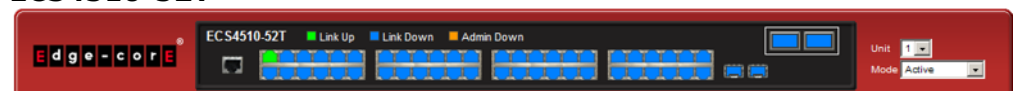
ECS4510-28P



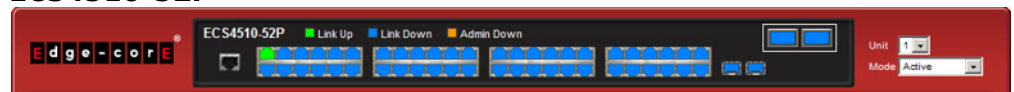
ECS4510-28F



ECS4510-52T



ECS4510-52P



MAIN MENU Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 6: Switch Main Menu

Menu	Description	Page
System		
General	Provides basic system description, including contact information	120
Switch	Shows the number of ports, hardware version, power status, and firmware version numbers	121
Capability	Enables support for jumbo frames; shows the bridge extension parameters	122, 123
File		125
Copy	Allows the transfer and copying files	125
Set Startup	Sets the startup file	128
Show	Shows the files stored in flash memory; allows deletion of files	129
Automatic Operation Code Upgrade	Automatically upgrades operation code if a newer version is found on the server	130
Time		134
Configure General		
Manual	Manually sets the current time	134
SNTP	Configures SNTP polling interval	135
NTP	Configures NTP authentication parameters	136
Configure Time Server	Configures a list of SNTP servers	137
Configure SNTP Server	Sets the IP address for SNTP time servers	137
Add NTP Server	Adds NTP time server and index of authentication key	138
Show NTP Server	Shows list of configured NTP time servers	138
Add NTP Authentication Key	Adds key index and corresponding MD5 key	139
Show NTP Authentication Key	Shows list of configured authentication keys	139
Configure Time Zone	Sets the local time zone for the system clock	141
Console	Sets console port connection parameters	142
Telnet	Sets Telnet connection parameters	144
CPU Utilization	Displays information on CPU utilization	145
Memory Status	Shows memory utilization parameters	146
Reset	Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval	147
Interface		151
Port		151
General		151
Configure by Port List	Configures connection settings per port	151
Configure by Port Range	Configures connection settings for a range of ports	154

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Information	Displays port connection status	155
Mirror		156
Add	Sets the source and target ports for mirroring	156
Show	Shows the configured mirror sessions	156
Statistics	Shows Interface, Etherlike, and RMON port statistics	162
Chart	Shows Interface, Etherlike, and RMON port statistics	162
Cable Test	Performs cable diagnostics for selected port to diagnose any cable faults (short, open etc.) and report the cable length	166
Trunk		168
Static		169
Configure Trunk		169
Add	Creates a trunk, along with the first port member	169
Show	Shows the configured trunk identifiers	169
Add Member	Specifies ports to group into static trunks	169
Show Member	Shows the port members for the selected trunk	169
Configure General		169
Configure	Configures trunk connection settings	169
Show Information	Displays trunk connection settings	169
Dynamic		172
Configure Aggregator	Configures administration key and timeout for specific LACP groups	172
Configure Aggregation Port		169
Configure		169
General	Allows ports to dynamically join trunks	172
Actor	Configures parameters for link aggregation group members on the local side	172
Partner	Configures parameters for link aggregation group members on the remote side	172
Show Information		178
Counters	Displays statistics for LACP protocol messages	178
Internal	Displays configuration settings and operational state for the local side of a link aggregation	179
Neighbors	Displays configuration settings and operational state for the remote side of a link aggregation	181
Configure Trunk		172
Configure	Configures connection settings	172
Show	Displays port connection status	172
Show Member	Shows the active members in a trunk	172
Statistics	Shows Interface, Etherlike, and RMON port statistics	162

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Chart	Shows Interface, Etherlike, and RMON port statistics	162
Green Ethernet	Adjusts the power provided to ports based on the length of the cable used to connect to other devices	182
RSPAN	Mirrors traffic from remote switches for analysis at a destination port on the local switch	158
sFlow	Configures flow sampling for source and destination ports	184
Configure Global	Enables sFlow globally for the switch	185
Configure Interface	Configures flow sampling for source and destination ports	185
Traffic Segmentation		187
Configure Global	Enables traffic segmentation globally	187
Configure Session	Configures the uplink and down-link ports for a segmented group of ports	189
VLAN Trunking	Allows unknown VLAN groups to pass through the specified interface	191
VLAN	Virtual LAN	193
Static		
Add	Creates VLAN groups	196
Show	Displays configured VLAN groups	196
Modify	Configures group name and administrative status	196
Edit Member by VLAN	Specifies VLAN attributes per VLAN	199
Edit Member by Interface	Specifies VLAN attributes per interface	199
Edit Member by Interface Range	Specifies VLAN attributes per interface range	199
Dynamic		
Configure General	Enables GVRP VLAN registration protocol globally	203
Configure Interface	Configures GVRP status and timers per interface	203
Show Dynamic VLAN		203
Show VLAN	Shows the VLANs this switch has joined through GVRP	203
Show VLAN Member	Shows the interfaces assigned to a VLAN through GVRP	203
Tunnel	IEEE 802.1Q (QinQ) Tunneling	206
Configure Global	Sets tunnel mode for the switch	210
Configure Service	Sets a CVLAN to SPVLAN mapping entry	211
Configure Interface	Sets the tunnel mode for any participating interface	213
Protocol		215
Configure Protocol		215
Add	Creates a protocol group, specifying supported protocols	215
Show	Shows configured protocol groups	215
Configure Interface		217
Add	Maps a protocol group to a VLAN	217

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show	Shows the protocol groups mapped to each VLAN	217
IP Subnet		219
Add	Maps IP subnet traffic to a VLAN	219
Show	Shows IP subnet to VLAN mapping	219
MAC-Based		221
Add	Maps traffic with specified source MAC address to a VLAN	221
Show	Shows source MAC address to VLAN mapping	221
Mirror		223
Add	Mirrors traffic from one or more source VLANs to a target port	223
Show	Shows mirror list	223
Translation		224
Add	Maps VLAN IDs between the customer and service provider	224
Show	Displays the configuration settings for VLAN translation	224
MAC Address		227
Static		227
Add	Configures static entries in the address table	227
Show	Displays static entries in the address table	227
Dynamic		
Configure Aging	Sets timeout for dynamically learned entries	229
Show Dynamic MAC	Displays dynamic entries in the address table	230
Clear Dynamic MAC	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries	231
Mirror	Mirrors traffic matching a specified source address from any port on the switch to a target port	232
Spanning Tree		235
Loopback Detection	Configures Loopback Detection parameters	238
STA	Spanning Tree Algorithm	
Configure Global		
Configure	Configures global bridge settings for STP, RSTP and MSTP	240
Show Information	Displays STA values used for the bridge	245
Configure Interface		
Configure	Configures interface settings for STA	246
Show Information	Displays interface settings for STA	250
MSTP	Multiple Spanning Tree Algorithm	253
Configure Global		253
Add	Configures initial VLAN and priority for an MST instance	253
Modify	Configures the priority or an MST instance	253

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show	Configures global settings for an MST instance	253
Add Member	Adds VLAN members for an MST instance	253
Show Member	Adds or deletes VLAN members for an MST instance	253
Show Information	Displays MSTP values used for the bridge	
Configure Interface		257
Configure	Configures interface settings for an MST instance	257
Show Information	Displays interface settings for an MST instance	257
Traffic		
Rate Limit	Sets the input and output rate limits for a port	259
Storm Control	Sets the broadcast storm threshold for each interface	260
Auto Traffic Control	Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port	263
Configure Global	Sets the time to apply the control response after traffic has exceeded the upper threshold, and the time to release the control response after traffic has fallen beneath the lower threshold	264
Configure Interface	Sets the storm control mode (broadcast or multicast), the traffic thresholds, the control response, to automatically release a response of rate limiting, or to send related SNMP trap messages	266
Priority		
Default Priority	Sets the default priority for each port or trunk	269
Queue	Sets queue mode for the switch; sets the service weight for each queue that will use a weighted or hybrid mode	270
Trust Mode	Selects DSCP or CoS priority processing	276
DSCP to DSCP		277
Add	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	277
Show	Shows the DSCP to DSCP mapping list	277
CoS to DSCP		280
Add	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing	280
Show	Shows the CoS to DSCP mapping list	280
PHB to Queue		273
Add	Maps internal per-hop behavior values to hardware queues	273
Show	Shows the PHB to Queue mapping list	273
DiffServ		283
Configure Class		284
Add	Creates a class map for a type of traffic	284
Show	Shows configured class maps	284
Modify	Modifies the name of a class map	284
Add Rule	Configures the criteria used to classify ingress traffic	284
Show Rule	Shows the traffic classification rules for a class map	284

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Policy		287
Add	Creates a policy map to apply to multiple interfaces	287
Show	Shows configured policy maps	287
Modify	Modifies the name of a policy map	287
Add Rule	Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic	287
Show Rule	Shows the rules used to enforce bandwidth policing for a policy map	287
Configure Interface	Applies a policy map to an ingress port	297
VoIP	Voice over IP	299
Configure Global	Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time	299
Configure OUI		301
Add	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	301
Show	Shows the OUI telephony list	301
Configure Interface	Configures VoIP traffic settings for ports, including the way in which a port is added to the Voice VLAN, filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to the voice traffic	302
Security		305
AAA	Authentication, Authorization and Accounting	306
System Authentication	Configures authentication sequence – local, RADIUS, and TACACS	307
Server		308
Configure Server	Configures RADIUS and TACACS server message exchange settings	308
Configure Group		308
Add	Specifies a group of authentication servers and sets the priority sequence	308
Show	Shows the authentication server groups and priority sequence	308
Accounting	Enables accounting of requested services for billing or security purposes	313
Configure Global	Specifies the interval at which the local accounting service updates information to the accounting server	313
Configure Method		313
Add	Configures accounting for various service types	313
Show	Shows the accounting settings used for various service types	313
Configure Service	Sets the accounting method applied to specific interfaces for 802.1X, CLI command privilege levels for the console port, and for Telnet	313
Show Information		313
Summary	Shows the configured accounting methods, and the methods applied to specific interfaces	313
Statistics	Shows basic accounting information recorded for user sessions	313

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Authorization	Enables authorization of requested services	319
Configure Method		319
Add	Configures authorization for various service types	319
Show	Shows the authorization settings used for various service types	319
Configure Service	Sets the authorization method applied used for the console port, and for Telnet	319
Show Information	Shows the configured authorization methods, and the methods applied to specific interfaces	319
User Accounts		322
Add	Configures user names, passwords, and access levels	322
Show	Shows authorized users	322
Modify	Modifies user attributes	322
Web Authentication	Allows authentication and access to the network when 802.1X or Network Access authentication are infeasible or impractical	324
Configure Global	Configures general protocol settings	324
Configure Interface	Enables Web Authentication for individual ports	325
Network Access	MAC address-based network access authentication	326
Configure Global	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	329
Configure Interface		330
General	Enables MAC authentication on a port; sets the maximum number of address that can be authenticated, the guest VLAN, dynamic VLAN and dynamic QoS	330
Link Detection	Configures detection of changes in link status, and the response (i.e., send trap or shut down port)	332
Configure MAC Filter		333
Add	Specifies MAC addresses exempt from authentication	333
Show	Shows the list of exempt MAC addresses	333
Show Information	Shows the authenticated MAC address list	335
HTTPS	Secure HTTP	336
Configure Global	Enables HTTPSs, and specifies the UDP port to use	336
Copy Certificate	Replaces the default secure-site certificate	338
SSH	Secure Shell	340
Configure Global	Configures SSH server settings	342
Configure Host Key		344
Generate	Generates the host key pair (public and private)	344
Show	Displays RSA and DSA host keys; deletes host keys	344
Configure User Key		345
Copy	Imports user public keys from TFTP server	345
Show	Displays RSA and DSA user keys; deletes user keys	345

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
ACL	Access Control Lists	347
Configure Time Range	Configures the time to apply an ACL	349
Add	Specifies the name of a time range	349
Show	Shows the name of configured time ranges	349
Add Rule		349
Absolute	Sets exact time or time range	349
Periodic	Sets a recurrent time	349
Show Rule	Shows the time specified by a rule	349
Configure ACL		352
Show TCAM	Shows utilization parameters for TCAM	351
Add	Adds an ACL based on IP or MAC address filtering	352
Show	Shows the name and type of configured ACLs	352
Add Rule	Configures packet filtering based on IP or MAC addresses and other packet attributes	352
Show Rule	Shows the rules specified for an ACL	352
Configure Interface	Binds a port to the specified ACL and time range	
Configure	Binds a port to the specified ACL and time range	366
Add Mirror	MIrrors matching traffic to the specified port	367
Show Mirror	Shows ACLs mirrored to specified port	367
Show Hardware Counters	Shows statistics for ACL hardware counters	369
ARP Inspection		370
Configure General	Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection	371
Configure VLAN	Enables ARP inspection on specified VLANs	373
Configure Interface	Sets the trust mode for ports, and sets the rate limit for packet inspection	375
Show Information		376
Show Statistics	Displays statistics on the inspection process	376
Show Log	Shows the inspection log list	377
IP Filter		378
Add	Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet	378
Show	Shows the addresses to be allowed management access	378
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	380
Port Authentication	IEEE 802.1X	382
Configure Global	Enables authentication and EAPOL pass-through	384
Configure Interface	Sets authentication parameters for individual ports	385
Show Statistics	Displays protocol statistics for the selected port	391

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
DoS Protection	Protects against Denial-of-Service attacks	394
IP Source Guard	Filters IP traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table	396
Port Configuration	Enables IP source guard and selects filter type per port	397
Static Binding		399
Add	Adds a static addresses to the source-guard binding table	399
Show	Shows static addresses in the source-guard binding table	399
Dynamic Binding	Displays the source-guard binding table for a selected interface	401
Administration		411
Log		412
System		412
Configure Global	Stores error messages in local memory	412
Show System Logs	Shows logged error messages	412
Remote	Configures the logging of messages to a remote logging process	414
SMTP	Sends an SMTP client message to a participating server	415
LLDP		416
Configure Global	Configures global LLDP timing parameters	417
Configure Interface		419
Configure General	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise	419
Add CA-Type	Specifies the physical location of the device attached to an interface	422
Show Local Device Information		424
General	Displays general information about the local device	424
Port/Trunk	Displays information about each interface	424
Show Remote Device Information		428
Port/Trunk	Displays information about a remote device connected to a port on this switch	428
Port/Trunk Details	Displays detailed information about a remote device connected to this switch	428
Show Device Statistics		436
General	Displays statistics for all connected remote devices	436
Port/Trunk	Displays statistics for remote devices on a selected port or trunk	436
PoE*	Power over Ethernet	438
Configure Global	Displays the power budget for the switch	439
Configure Interface	Configures port power parameters	440
SNMP	Simple Network Management Protocol	442
Configure Global	Enables SNMP agent status, and sets related trap functions	444

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Engine		445
Set Engine ID	Sets the SNMP v3 engine ID on this switch	445
Add Remote Engine	Sets the SNMP v3 engine ID for a remote device	446
Show Remote Engine	Shows configured engine ID for remote devices	446
Configure View		448
Add View	Adds an SNMP v3 view of the OID MIB	448
Show View	Shows configured SNMP v3 views	448
Add OID Subtree	Specifies a part of the subtree for the selected view	448
Show OID Subtree	Shows the subtrees assigned to each view	448
Configure Group		451
Add	Adds a group with access policies for assigned users	451
Show	Shows configured groups and access policies	451
Configure User		
Add Community	Configures community strings and access mode	456
Show Community	Shows community strings and access mode	456
Add SNMPv3 Local User	Configures SNMPv3 users on this switch	457
Show SNMPv3 Local User	Shows SNMPv3 users configured on this switch	457
Change SNMPv3 Local User Group	Assign a local user to a new group	457
Add SNMPv3 Remote User	Configures SNMPv3 users from a remote device	459
Show SNMPv3 Remote User	Shows SNMPv3 users set from a remote device	457
Configure Trap		462
Add	Configures trap managers to receive messages on key events that occur this switch	462
Show	Shows configured trap managers	462
Configure Notify Filter		
Add	Creates an SNMP notification log	466
Show	Shows the configured notification logs	466
Show Statistics	Shows the status of SNMP communications	468
RMON	Remote Monitoring	470
Configure Global		
Add		
Alarm	Sets threshold bounds for a monitored variable	471
Event	Creates a response event for an alarm	473
Show		471
Alarm	Shows all configured alarms	471
Event	Shows all configured events	473

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Interface		
Add		
History	Periodically samples statistics on a physical interface	475
Statistics	Enables collection of statistics on a physical interface	478
Show		
History	Shows sampling parameters for each entry in the history group	475
Statistics	Shows sampling parameters for each entry in the statistics group	478
Show Details		
History	Shows sampled data for each entry in the history group	475
Statistics	Shows sampled data for each entry in the history group	478
Cluster		481
Configure Global	Globally enables clustering for the switch; sets Commander status	481
Configure Member	Adds switch Members to the cluster	483
Show Member	Shows cluster switch member; managed switch members	484
ERPS	Ethernet Ring Protection Switching	485
Configure Global	Activates ERPS globally	489
Configure Domain		490
Add	Creates an ERPS ring	490
Show	Shows list of configured ERPS rings, status, and settings	490
Configure Details	Configures ring parameters	490
Configure Operation	Blocks a ring port using Forced Switch or Manual Switch commands	506
CFM	Connectivity Fault Management	510
Configure Global	Configures global settings, including administrative status, cross-check start delay, link trace, and SNMP traps	513
Configure Interface	Configures administrative status on an interface	517
Configure MD	Configure Maintenance Domains	517
Add	Defines a portion of the network for which connectivity faults can be managed, identified by an MD index, maintenance level, and the MIP creation method	517
Configure Details	Configures the archive hold time and fault notification settings	517
Show	Shows list of configured maintenance domains	517
Configure MA	Configure Maintenance Associations	522
Add	Defines a unique CFM service instance, identified by its parent MD, the MA index, the VLAN assigned to the MA, and the MIP creation method	522
Configure Details	Configures detailed settings, including continuity check status and interval level, cross-check status, and alarm indication signal parameters	522
Show	Shows list of configured maintenance associations	522

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure MEP	Configures Maintenance End Points	527
Add	Configures MEPs at the domain boundary to provide management access for each maintenance association	527
Show	Shows list of configured maintenance end points	527
Configure Remote MEP	Configures Remote Maintenance End Points	528
Add	Configures a static list of remote MEPs for comparison against the MEPs learned through continuity check messages	528
Show	Shows list of configured remote maintenance end points	528
Transmit Link Trace	Sends link trace messages to isolate connectivity faults by tracing the path through a network to the designated target node	530
Transmit Loopback	Sends loopback messages to isolate connectivity faults by requesting a target node to echo the message back to the source	532
Transmit Delay Measure	Sends periodic delay-measure requests to a specified MEP within a maintenance association	534
Show Information		
Show Local MEP	Shows the MEPs configured on this device	536
Show Local MEP Details	Displays detailed CFM information about a specified local MEP in the continuity check database	537
Show Local MIP	Shows the MIPs on this device discovered by the CFM protocol	539
Show Remote MEP	Shows MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database	540
Show Remote MEP Details	Displays detailed CFM information about a specified remote MEP in the continuity check database	541
Show Link Trace Cache	Shows information about link trace operations launched from this device	543
Show Fault Notification Generator	Displays configuration settings for the fault notification generator	544
Show Continuity Check Error	Displays CFM continuity check errors logged on this device	545
OAM	Operation, Administration, and Maintenance	547
Interface	Enables OAM on specified port, sets the mode to active or passive, and enables the reporting of critical events or errored frame events	547
Counters	Displays statistics on OAM PDUs	549
Event Log	Displays the log for recorded link events	550
Remote Interface	Displays information about attached OAM-enabled devices	551
Remote Loopback	Performs a loopback test on the specified port	552
IP		617
General		
Routing Interface		
Configure Interface		
Add Address	Configures an IP interface for a VLAN	617
Show Address	Shows the IP interfaces assigned to a VLAN	617

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Ping	Sends ICMP echo request packets to another node on the network	659
Trace Route	Shows the route packets take to the specified destination	660
ARP	Address Resolution Protocol	661
Configure General	Sets the aging time for dynamic entries in the ARP cache	662
Configure Static Address		664
Add	Statically maps a physical address to an IP address	664
Show	Shows the MAC to IP address static table	664
Show Information	Shows entries in the Address Resolution Protocol (ARP) cache	
Dynamic Address	Shows dynamically learned entries in the IP routing table	665
Other Address	Shows internal addresses used by the switch	665
Statistics	Shows statistics on ARP requests sent and received	666
Routing		
Static Routes		667
Add	Configures static routing entries	667
Show	Shows static routing entries	667
Routing Table		
Show Information	Shows all routing entries, including local, static and dynamic routes	669
IPv6 Configuration		621
Configure Global	Sets an IPv6 default gateway for traffic with no known next hop	621
Configure Interface	Configures IPv6 interface address using auto-configuration or link-local address, and sets related protocol settings	622
Add IPv6 Address	Adds an global unicast, EUI-64, or link-local IPv6 address to an interface	627
Show IPv6 Address	Show the IPv6 addresses assigned to an interface	630
Show IPv6 Neighbor Cache	Displays information in the IPv6 neighbor discovery cache	631
Show Statistics		633
IPv6	Shows statistics about IPv6 traffic	633
ICMPv6	Shows statistics about ICMPv6 messages	633
UDP	Shows statistics about UDP messages	633
Show MTU	Shows 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	638
IP Service		639
DNS	Domain Name Service	639
General		639
Configure Global	Enables DNS lookup; defines the default domain name appended to incomplete host names	639

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Add Domain Name	Defines a list of domain names that can be appended to incomplete host names	640
Show Domain Names	Shows the configured domain name list	640
Add Name Server	Specifies IP address of name servers for dynamic lookup	642
Show Name Servers	Shows the name server address list	642
Static Host Table		643
Add	Configures static entries for domain name to address mapping	643
Show	Shows the list of static mapping entries	643
Modify	Modifies the static address mapped to the selected host name	643
Cache	Displays cache entries discovered by designated name servers	644
DHCP	Dynamic Host Configuration Protocol	645
Client	Specifies the DHCP client identifier for an interface	645
Relay	Specifies DHCP relay servers	647
Snooping		402
Configure Global	Enables DHCP snooping globally, MAC-address verification, information option; and sets the information policy	404
Configure VLAN	Enables DHCP snooping on a VLAN	406
Configure Interface	Sets the trust mode for an interface	407
Show Information	Displays the DHCP Snooping binding information	408
PPPoE Intermediate Agent	Point-to-Point Protocol over Ethernet Intermediate Agent	648
Configure Global	Enables PPPoE IA on the switch, sets access node identifier, sets generic error message	648
Configure Interface	Enables PPPoE IA on an interface, sets trust status, enables vendor tag stripping, sets circuit ID and remote ID	650
Show Statistics	Shows statistics on PPPoE IA protocol messages	652
Multicast		557
IGMP Snooping		558
General	Enables multicast filtering; configures parameters for multicast snooping	560
Multicast Router		564
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	564
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	564
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	564
IGMP Member		566
Add Static Member	Statically assigns multicast addresses to the selected VLAN	566
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	566

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Interface		568
Configure VLAN	Configures IGMP snooping per VLAN interface	568
Show VLAN Information	Shows IGMP snooping settings per VLAN interface	568
Configure Port	Configures the interface to drop IGMP query packets or all multicast data packets	573
Configure Trunk	Configures the interface to drop IGMP query packets or all multicast data packets	573
Forwarding Entry	Displays the current multicast groups learned through IGMP Snooping	574
Filter		579
Configure General	Enables IGMP filtering for the switch	579
Configure Profile		580
Add	Adds IGMP filter profile; and sets access mode	580
Show	Shows configured IGMP filter profiles	580
Add Multicast Group Range	Assigns multicast groups to selected profile	580
Show Multicast Group Range	Shows multicast groups assigned to a profile	580
Configure Interface	Assigns IGMP filter profiles to port interfaces and sets throttling action	582
Statistics		575
Show Query Statistics	Shows statistics for query-related messages	575
Show VLAN Statistics	Shows statistics for protocol messages, number of active groups	575
Show Port Statistics	Shows statistics for protocol messages, number of active groups	575
Show Trunk Statistics	Shows statistics for protocol messages, number of active groups	575
MVR	Multicast VLAN Registration	584
Configure Global	Configures proxy switching and robustness value	585
Configure Domain	Enables MVR for a domain, sets the MVR VLAN, forwarding priority, and upstream source IP	587
Configure Profile		589
Add	Configures multicast stream addresses	589
Show	Shows multicast stream addresses	589
Associate Profile		589
Add	Maps an address profile to a domain	589
Show	Shows addresses profile to domain mapping	589
Configure Interface	Configures MVR interface type and immediate leave mode; also displays MVR operational and active status	592
Configure Static Group Member		594
Add	Statically assigns MVR multicast streams to an interface	594
Show	Shows MVR multicast streams assigned to an interface	594
Show Member	Shows the multicast groups assigned to an MVR VLAN, the source address of the multicast services, and the interfaces with active subscribers	596

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Statistics		597
Show Query Statistics	Shows statistics for query-related messages	597
Show VLAN Statistics	Shows statistics for protocol messages and number of active groups	597
Show Port Statistics	Shows statistics for protocol messages and number of active groups	597
Show Trunk Statistics	Shows statistics for protocol messages and number of active groups	597
MVR6	Multicast VLAN Registration for IPv6	601
Configure Global	Configures proxy switching and robustness value	602
Configure Domain	Enables MVR for a domain, sets the MVR VLAN, forwarding priority, and upstream source IP	604
Configure Profile		605
Add	Configures multicast stream addresses	605
Show	Shows multicast stream addresses	605
Associate Profile		605
Add	Maps an address profile to a domain	605
Show	Shows addresses profile to domain mapping	605
Configure Interface	Configures MVR interface type and immediate leave mode; also displays MVR operational and active status	608
Configure Port	Configures MVR attributes for a port	608
Configure Trunk	Configures MVR attributes for a trunk	608
Configure Static Group Member		610
Add	Statically assigns MVR multicast streams to an interface	610
Show	Shows MVR multicast streams assigned to an interface	610
Show Member	Shows the multicast groups assigned to an MVR VLAN, the source address of the multicast services, and the interfaces with active subscribers	612
Show Statistics		613
Show Query Statistics	Shows statistics for query-related messages	613
Show VLAN Statistics	Shows statistics for protocol messages, number of active groups	613
Show Port Statistics	Shows statistics for protocol messages, number of active groups	613
Show Trunk Statistics	Shows statistics for protocol messages, number of active groups	613
Routing Protocol		
RIP		672
General		673
Configure	Enables or disables RIP, sets the global RIP attributes and timer values	673
Clear Route	Clears the specified route type or network interface from the routing table	676

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Network		677
Add	Sets the network interfaces that will use RIP	677
Show	Shows the network interfaces that will use RIP	677
Passive Interface		679
Add	Stops RIP broadcast and multicast messages from being sent on specified network interfaces	679
Show	Shows the configured passive interfaces	679
Neighbor Address		680
Add	Configures the router to directly exchange routing information with a static neighbor	680
Show	Shows adjacent hosts or interfaces configured as a neighboring router	680
Redistribute		681
Add	Imports external routing information from other routing domains (that is, protocols) into the autonomous system	681
Show	Shows the external routing information to be imported from other routing domains	681
Distance		683
Add	Defines an administrative distance for external routes learned from other routing protocols	683
Show	Shows the administrative distances assigned to external routes learned from other routing protocols	683
Interface		685
Add	Configures RIP parameters for each interface, including send and receive versions, authentication, and method of loopback prevention	685
Show	Shows the RIP parameters set for each interface	685
Modify	Modifies RIP parameters for an interface	685
Statistics		
Show Interface Information	Shows RIP settings, and statistics on RIP protocol messages	689
Show Peer Information	Displays information on neighboring RIP routers	689
Reset Statistics	Clears statistics for RIP protocol messages	690

* ECS4510-28P/52P

This chapter describes the following topics:

- ◆ [Displaying System Information](#) – Provides basic system description, including contact information.
- ◆ [Displaying Hardware/Software Versions](#) – Shows the hardware version, power status, and firmware versions
- ◆ [Configuring Support for Jumbo Frames](#) – Enables support for jumbo frames.
- ◆ [Displaying Bridge Extension Capabilities](#) – Shows the bridge extension parameters.
- ◆ [Managing System Files](#) – Describes how to upgrade operating software or configuration files, and set the system start-up files.
- ◆ [Setting the System Clock](#) – Sets the current time manually or through specified NTP or SNTP servers.
- ◆ [Configuring the Console Port](#) – Sets console port connection parameters.
- ◆ [Configuring Telnet Settings](#) – Sets Telnet connection parameters.
- ◆ [Displaying CPU Utilization](#) – Displays information on CPU utilization.
- ◆ [Displaying Memory Utilization](#) – Shows memory utilization parameters.
- ◆ [Resetting the System](#) – Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

DISPLAYING SYSTEM INFORMATION

Use the System > General page to identify the system by displaying information such as the device name, location and contact information.

CLI REFERENCES

- ◆ "System Management Commands" on page 715
- ◆ "SNMP Commands" on page 785

PARAMETERS

These parameters are displayed:

- ◆ **System Description** – Brief description of device type.
- ◆ **System Object ID** – 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.

WEB INTERFACE

To configure general system information:

1. Click System, General.
2. Specify the system name, location, and contact information for the system administrator.
3. Click Apply.

Figure 3: System Information

The screenshot shows a web interface titled "System > General". It contains a table with system information fields. The fields are: System Description (ECS4510-28T), System Object ID (1.3.6.1.4.1.259.10.1.24.1), System Up Time (0 days, 1 hours, 8 minutes, and 10.84 seconds), System Name (empty text box), System Location (empty text box), and System Contact (empty text box). At the bottom right, there are two buttons: "Apply" and "Revert".

System > General	
System Description	ECS4510-28T
System Object ID	1.3.6.1.4.1.259.10.1.24.1
System Up Time	0 days, 1 hours, 8 minutes, and 10.84 seconds
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

DISPLAYING HARDWARE/SOFTWARE VERSIONS

Use the System > Switch page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

CLI REFERENCES

- ◆ ["System Management Commands" on page 715](#)

PARAMETERS

The following parameters are displayed:

Main Board Information

- ◆ **Serial Number** – The serial number of the switch.
- ◆ **Number of Ports** – Number of built-in ports.
- ◆ **Hardware Version** – Hardware version of the main board.
- ◆ **Main Power Status** – Displays the status of the internal power supply.
- ◆ **Redundant Power Status** – Displays the status of the redundant power supply.

Management Software Information

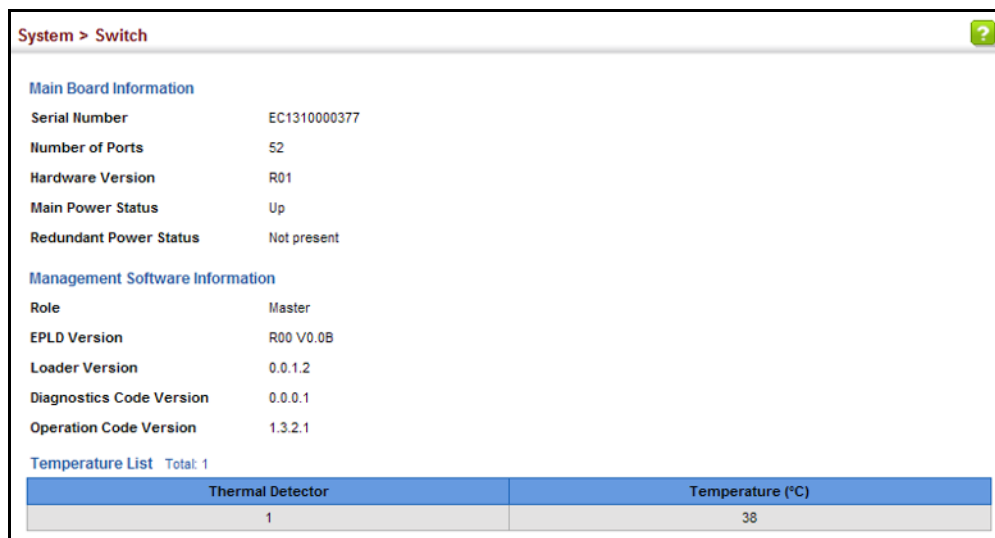
- ◆ **Role** – Shows that this switch is operating as Master or Slave.
- ◆ **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- ◆ **Loader Version** – Version number of loader code.
- ◆ **Diagnostics Code Version** – Version of Power-On Self-Test (POST) and boot code.
- ◆ **Operation Code Version** – Version number of runtime code.
- ◆ **Thermal Detector** – The detector is near the back of the unit.
- ◆ **Temperature** – Temperature at specified thermal detection point.

WEB INTERFACE

To view hardware and software version information.

1. Click System, then Switch.

Figure 4: General Switch Information



Main Board Information	
Serial Number	EC1310000377
Number of Ports	52
Hardware Version	R01
Main Power Status	Up
Redundant Power Status	Not present
Management Software Information	
Role	Master
EPLD Version	R00 V0.0B
Loader Version	0.0.1.2
Diagnostics Code Version	0.0.0.1
Operation Code Version	1.3.2.1
Temperature List Total: 1	
Thermal Detector	Temperature (°C)
1	38

CONFIGURING SUPPORT FOR JUMBO FRAMES

Use the System > Capability page to configure support for layer 2 jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes for Gigabit Ethernet and 10 Gigabit Ethernet ports or trunks. 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.

CLI REFERENCES

- ◆ ["System Management Commands" on page 715](#)

USAGE GUIDELINES

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.

PARAMETERS

The following parameters are displayed:

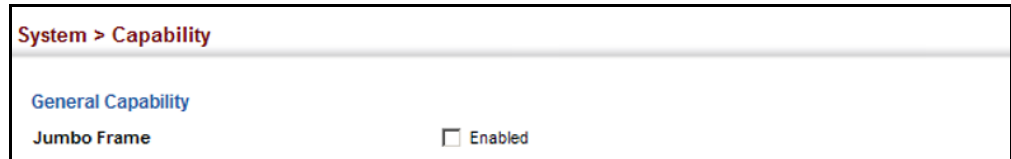
- ◆ **Jumbo Frame** – Configures support for jumbo frames.
(Default: Disabled)

WEB INTERFACE

To configure support for jumbo frames:

1. Click System, then Capability.
2. Enable or disable support for jumbo frames.
3. Click Apply.

Figure 5: Configuring Support for Jumbo Frames



DISPLAYING BRIDGE EXTENSION CAPABILITIES

Use the System > Capability page to display settings based on the Bridge MIB. The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

CLI REFERENCES

- ◆ ["GVRP and Bridge Extension Commands" on page 1120](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- ◆ **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to ["Class of Service" on page 269.](#))
- ◆ **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to ["Setting Static Addresses" on page 227.](#))
- ◆ **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.
- ◆ **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.

- ◆ **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 ["VLAN Configuration" on page 193.](#))
- ◆ **Max Supported VLAN Numbers** – The maximum number of VLANs supported on this switch.
- ◆ **Max Supported VLAN ID** – The maximum configurable VLAN identifier supported on this switch.
- ◆ **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

WEB INTERFACE

To view Bridge Extension information:

1. Click System, then Capability.

Figure 6: Displaying Bridge Extension Configuration

The screenshot displays the 'System > Capability' configuration page. It features a table of settings under the 'Bridge Extension' section. The 'Jumbo Frame' setting is under 'General Capability' and is currently disabled. The 'Bridge Extension' section includes settings for 'Extended Multicast Filtering Services' (No), 'Traffic Classes' (Enabled), 'Static Entry Individual Port' (Yes), 'VLAN Version Number' (1), 'VLAN Learning' (VL), 'Local VLAN Capable' (No), 'Configurable PVID Tagging' (Yes), 'Max Supported VLAN Numbers' (4093), 'Max Supported VLAN ID' (4093), and 'GMRP' (Disabled). 'Apply' and 'Revert' buttons are at the bottom right.

System > Capability	
General Capability	
Jumbo Frame	<input type="checkbox"/> Enabled
Bridge Extension	
Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Version Number	1
VLAN Learning	VL
Local VLAN Capable	No
Configurable PVID Tagging	Yes
Max Supported VLAN Numbers	4093
Max Supported VLAN ID	4093
GMRP	Disabled
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

MANAGING SYSTEM FILES

This section describes how to upgrade the switch operating software or configuration files, and set the system start-up files.

COPYING FILES VIA FTP/TFTP OR HTTP

Use the System > File (Copy) page to upload/download firmware or configuration settings using FTP, TFTP or HTTP. By backing up a file to an FTP/TFTP server or management station, that file can later be downloaded to the switch to restore operation. Specify the method of file transfer, along with the file type and file names as required.

You can also set the switch to use new firmware or configuration settings without overwriting the current version. Just download the file using a different name from the current version, and then set the new file as the startup file.

CLI REFERENCES

- ◆ ["copy" on page 736](#)

COMMAND USAGE

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.

PARAMETERS

The following parameters are displayed:

- ◆ **Copy Type** – The firmware copy operation includes these options:
 - FTP Upgrade – Copies a file from an FTP server to the switch.
 - FTP Download – Copies a file from the switch to an FTP server.
 - HTTP Upgrade – Copies a file from a management station to the switch.
 - HTTP Download – Copies a file from the switch to a management station
 - TFTP Upgrade – Copies a file from a TFTP server to the switch.
 - TFTP Download – Copies a file from the switch to a TFTP server.
- ◆ **FTP/TFTP Server IP Address** – The IP address of an FTP/TFTP server.
- ◆ **User Name** – The user name for FTP server access.
- ◆ **Password** – The password for FTP server access.
- ◆ **File Type** – Specify Operation Code to copy firmware.

- ◆ **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), 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, ".", "-", "_")



NOTE: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch.

NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

NOTE: The file “Factory_Default_Config.cfg” can be copied to a file server or management station, but cannot be used as the destination file name on the switch.

WEB INTERFACE

To copy firmware files:

1. Click System, then File.
2. Select Copy from the Action list.
3. Select FTP Upgrade, HTTP Upgrade, or TFTP Upgrade as the file transfer method.
4. If FTP or TFTP Upgrade is used, enter the IP address of the file server.
5. If FTP Upgrade is used, enter the user name and password for your account on the FTP server.
6. Set the file type to Operation Code.
7. Enter the name of the file to download.
8. Select a file on the switch to overwrite or specify a new file name.
9. Then click Apply.

Figure 7: Copy Firmware

If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SAVING THE RUNNING CONFIGURATION TO A LOCAL FILE

Use the System > File (Copy) page to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

CLI REFERENCES

- ◆ "copy" on page 736

PARAMETERS

The following parameters are displayed:

- ◆ **Copy Type** – The copy operation includes this option:
 - Running-Config – Copies the current configuration settings to a local file on the switch.
- ◆ **Destination File Name** – Copy to the currently designated startup file, or to a new file. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), 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, ".", "-", "_")



NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

WEB INTERFACE

To save the running configuration file:

1. Click System, then File.
2. Select Copy from the Action list.
3. Select Running-Config from the Copy Type list.
4. Select the current startup file on the switch to overwrite or specify a new file name.
5. Then click Apply.

Figure 8: Saving the Running Configuration



The screenshot shows a web interface for the 'System > File' configuration page. At the top, there is a breadcrumb 'System > File'. Below it, the 'Action' dropdown is set to 'Copy'. Under the 'Copy Type' section, the dropdown is set to 'Running-Config'. In the 'Destination File Name' section, there are two radio buttons. The first radio button is selected and is next to a dropdown menu showing 'startup1.cfg'. The second radio button is unselected and is next to an empty text input field. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SETTING THE START-UP FILE

Use the System > File (Set Start-Up) page to specify the firmware or configuration file to use for system initialization.

CLI REFERENCES

- ◆ ["whichboot" on page 740](#)
- ◆ ["boot system" on page 735](#)

WEB INTERFACE

To set a file to use for system initialization:

1. Click System, then File.
2. Select Set Start-Up from the Action list.
3. Mark the operation code or configuration file to be used at startup
4. Then click Apply.

Figure 9: Setting Start-Up Files

System > File

Action: Set Start-Up

File List Total: 3

	File Name	File Type	Start-Up	Size (bytes)
<input checked="" type="radio"/>	runtime.bix	Operation Code	Y	11354752
<input type="radio"/>	Factory_Default_Config.cfg	Config File	N	455
<input checked="" type="radio"/>	startup1.cfg	Config File	Y	2297

Apply Revert

To start using the new firmware or configuration settings, reboot the system via the System > Reset menu.

SHOWING SYSTEM FILES

Use the System > File (Show) page to show the files in the system directory, or to delete a file.



NOTE: Files designated for start-up, and the Factory_Default_Config.cfg file, cannot be deleted.

CLI REFERENCES

- ◆ "dir" on page 739
- ◆ "delete" on page 739

WEB INTERFACE

To show the system files:

1. Click System, then File.
2. Select Show from the Action list.
3. To delete a file, mark it in the File List and click Delete.

Figure 10: Displaying System Files

System > File

Action: Show

File List Total: 3

<input type="checkbox"/>	File Name	File Type	Start-Up	Size (bytes)
<input type="checkbox"/>	runtime.bix	Operation Code	Y	11354752
<input type="checkbox"/>	Factory_Default_Config.cfg	Config File	N	455
<input type="checkbox"/>	startup1.cfg	Config File	Y	2297

Delete Revert

AUTOMATIC OPERATION CODE UPGRADE

Use the System > File (Automatic Operation Code Upgrade) page to 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.

CLI REFERENCES

- ◆ "upgrade opcode auto" on page 741
- ◆ "upgrade opcode path" on page 742

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 *ECS4510-Series.bix* (using upper case and lower case letters exactly as indicated here). Enter the file name for other switches described in this manual exactly as shown on the web interface.
- ◆ 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 *ECS4510-SERIES.BIX* from the server even though *ECS4510-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, *ecs4510-series.bix* and *ECS4510-SERIES.bix* are considered to be unique files. Thus, if the upgrade file is stored as *ECS4510-SERIES.bix* (or even *EcS4510-SERIES.bix*) on a case-sensitive server, then the switch (requesting *ecs4510-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.

PARAMETERS

The following parameters are displayed:

- ◆ **Automatic Opcode Upgrade** – Enables the switch to search for an upgraded operation code file during the switch bootstrap process. (Default: Disabled)
- ◆ **Automatic Upgrade Location URL** – Defines where the switch should search for the operation code upgrade file. The last character of this URL must be a forward slash ("/"). The *ECS4510-Series.bix* filename must not be included since it is automatically appended by the switch. (Options: ftp, tftp)

The following syntax must be observed:

tftp://host[/filedir]/

- **tftp://** – Defines TFTP protocol for the server connection.
- **host** – Defines the IP address of the TFTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.
- **filedir** – Defines the directory, relative to the TFTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash "/".
- **/** – The forward slash must be the last character of the URL.

ftp://[username[:password@]]host[/filedir]/

- **ftp://** – Defines FTP protocol for the server connection.
- *username* – Defines the user name for the FTP connection. If the user name is omitted, then “anonymous” is the assumed user name for the connection.
- *password* – Defines the password for the FTP connection. To differentiate the password from the user name and host portions of the URL, a colon (:) must precede the password, and an “at” symbol (@), must follow the password. If the password is omitted, then “” (an empty string) is the assumed password for the connection.
- *host* – Defines the IP address of the FTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.
- *filedir* – Defines the directory, relative to the FTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash “/”.
- **/** – The forward slash must be the last character of the URL.

Examples

The following examples demonstrate the URL syntax for a TFTP server at IP address 192.168.0.1 with the operation code image stored in various locations:

- **tftp://192.168.0.1/**
The image file is in the TFTP root directory.
- **tftp://192.168.0.1/switch-opcode/**
The image file is in the “switch-opcode” directory, relative to the TFTP root.
- **tftp://192.168.0.1/switches/opcode/**
The image file is in the “opcode” directory, which is within the “switches” parent directory, relative to the TFTP root.

The following examples demonstrate the URL syntax for an FTP server at IP address 192.168.0.1 with various user name, password and file location options presented:

- **ftp://192.168.0.1/**
The user name and password are empty, so “anonymous” will be the user name and the password will be blank. The image file is in the FTP root directory.
- **ftp://switches:upgrade@192.168.0.1/**
The user name is “switches” and the password is “upgrade”. The image file is in the FTP root.

- ftp://switches:upgrade@192.168.0.1/switches/opcode/

The user name is "switches" and the password is "upgrade". The image file is in the "opcode" directory, which is within the "switches" parent directory, relative to the FTP root.

WEB INTERFACE

To configure automatic code upgrade:

1. Click System, then File.
2. Select Automatic Operation Code Upgrade from the Action list.
3. Mark the check box to enable Automatic Opcode Upgrade.
4. Enter the URL of the FTP or TFTP server, and the path and directory containing the operation code.
5. Click Apply.

Figure 11: Configuring Automatic Code Upgrade

System > File

Action: Automatic Operation Code Upgrade

Automatic Opcode Upgrade ☐ Enabled

Automatic Upgrade Location URL

Note: For automatic upgrades, the operation code file name must be set as ECS4510-Series.bix.

Apply Revert

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
.
.
.
```

SETTING THE SYSTEM CLOCK

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). 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, 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.

SETTING THE TIME MANUALLY Use the System > Time (Configure General - Manual) page to set the system time on the switch manually without using SNTP.

CLI REFERENCES

- ◆ ["calendar set" on page 775](#)
- ◆ ["show calendar" on page 776](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Current Time** – Shows the current time set on the switch.
- ◆ **Hours** – Sets the hour. (Range: 0-23)
- ◆ **Minutes** – Sets the minute value. (Range: 0-59)
- ◆ **Seconds** – Sets the second value. (Range: 0-59)
- ◆ **Month** – Sets the month. (Range: 1-12)
- ◆ **Day** – Sets the day of the month. (Range: 1-31)
- ◆ **Year** – Sets the year. (Range: 1970-2037)

WEB INTERFACE

To manually set the system clock:

1. Click System, then Time.
2. Select Configure General from the Step list.
3. Select Manual from the Maintain Type list.
4. Enter the time and date in the appropriate fields.
5. Click Apply

Figure 12: Manually Setting the System Clock

The screenshot shows a web interface for configuring the system time. At the top, it says "System > Time". Below that is a "Step:" dropdown menu set to "1. Configure General". The "Current Time" is displayed as "2011-9-26 7:53:34". Under "Maintain Type", a dropdown menu is set to "Manual". Below this are input fields for time: Hours (7), Minutes (53), Seconds (34), Month (9), Day (26), and Year (2011). At the bottom right are "Apply" and "Revert" buttons.

SETTING THE SNTP POLLING INTERVAL

Use the System > Time (Configure General - SNTP) page to set the polling interval at which the switch will query the specified time servers.

CLI REFERENCES

- ◆ ["Time" on page 767](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Current Time** – Shows the current time set on the switch.
- ◆ **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

WEB INTERFACE

To set the polling interval for SNTP:

1. Click System, then Time.
2. Select Configure General from the Step list.
3. Select SNTP from the Maintain Type list.
4. Modify the polling interval if required.
5. Click Apply

Figure 13: Setting the Polling Interval for SNTP

The screenshot shows a web interface for configuring system time. At the top, it says "System > Time". Below that is a "Step:" dropdown menu set to "1. Configure General". The "Current Time" is displayed as "2009-9-14 15:21:12". The "Maintain Type" is a dropdown menu set to "SNTP". Under the "SNTP Configuration" section, there is a field for "SNTP Polling Interval (16-16384)" with the value "16" entered, followed by "sec". At the bottom right are "Apply" and "Revert" buttons.

CONFIGURING NTP Use the System > Time (Configure General - NTP) page to configure NTP authentication and show the polling interval at which the switch will query the specified time servers.

CLI REFERENCES

- ◆ "Time" on page 767

PARAMETERS

The following parameters are displayed:

- ◆ **Current Time** – Shows the current time set on the switch.
- ◆ **Authentication Status** – Enables authentication for time requests and updates between the switch and NTP servers. (Default: Disabled)
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.
- ◆ **Polling Interval** – Shows the interval between sending requests for a time update from NTP servers. (Fixed: 1024 seconds)

WEB INTERFACE

To set the clock maintenance type to NTP:

1. Click System, then Time.
2. Select Configure General from the Step list.
3. Select NTP from the Maintain Type list.
4. Enable authentication if required.
5. Click Apply

Figure 14: Configuring NTP

System > Time

Step: 1. Configure General

Current Time 2011-9-26 7:57:29

Maintain Type NTP

NTP Configuration

Authentication Status ☒ Enabled

Polling Interval 1024 sec

Apply Revert

CONFIGURING TIME SERVERS Use the System > Time (Configure Time Server) pages to specify the IP address for NTP/SNTP time servers, or to set the authentication key for NTP time servers.

SPECIFYING SNTP TIME SERVERS

Use the System > Time (Configure Time Server – Configure SNTP Server) page to specify the IP address for up to three SNTP time servers.

CLI REFERENCES

- ◆ ["sntp server" on page 769](#)

PARAMETERS

The following parameters are displayed:

- ◆ **SNTP Server IP Address** – Sets the IPv4 or IPv6 address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

WEB INTERFACE

To set the SNTP time servers:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Configure SNTP Server from the Action list.
4. Enter the IP address of up to three time servers.
5. Click Apply.

Figure 15: Specifying SNTP Time Servers

The screenshot shows a web interface for configuring system time. At the top, it says "System > Time". Below that, there are two dropdown menus: "Step: 2. Configure Time Server" and "Action: Configure SNTP Server". Underneath, there are three text input fields labeled "SNTP Server IP Address 1", "SNTP Server IP Address 2", and "SNTP Server IP Address 3". The first field contains "10.1.0.19", the second contains "137.62.140.80", and the third contains "128.250.36.2". At the bottom right, there are two buttons: "Apply" and "Revert".

SPECIFYING NTP TIME SERVERS

Use the System > Time (Configure Time Server – Add NTP Server) page to add the IP address for up to 50 NTP time servers.

CLI REFERENCES

- ◆ ["ntp server" on page 773](#)

PARAMETERS

The following parameters are displayed:

- ◆ **NTP Server IP Address** – Adds the IPv4 or IPv6 address for up to 50 time servers. The switch will poll the specified time servers for updates when the clock maintenance type is set to NTP on the System > Time (Configure General) page. It issues time synchronization requests at a fixed interval of 1024 seconds. The switch 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.
- ◆ **Version** – Specifies the NTP version supported by the server.
(Fixed: Version 3)
- ◆ **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with the configured server. NTP authentication is optional. If enabled on the System > Time (Configure General) page, you must also configure at least one key on the System > Time (Add NTP Authentication Key) page.
(Range: 1-65535)

WEB INTERFACE

To add an NTP time server to the server list:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Add NTP Server from the Action list.
4. Enter the IP address of an NTP time server, and specify the index of the authentication key if authentication is required.
5. Click Apply.

Figure 16: Adding an NTP Time Server

System > Time

Step: 2. Configure Time Server Action: Add NTP Server

NTP Server IP Address: 192.168.3.20

Version: 3

Authentication Key (1-65535): 3 (optional)

Apply Revert

To show the list of configured NTP time servers:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Show NTP Server from the Action list.

Figure 17: Showing the NTP Time Server List

System > Time

Step: 2. Configure Time Server Action: Show NTP Server

NTP Server List Total: 1

	Server IP Address	Version	Authentication Key
<input type="checkbox"/>	192.168.3.20	3	3

Delete Revert

SPECIFYING NTP AUTHENTICATION KEYS

Use the System > Time (Configure Time Server – Add NTP Authentication Key) page to add an entry to the authentication key list.

CLI REFERENCES

- ◆ ["ntp authentication-key" on page 771](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with a configured server. NTP authentication is optional. When enabled on the System > Time (Configure General) page, you must also configure at least one key on this page. Up to 255 keys can be configured on the switch. (Range: 1-65535)
- ◆ **Key Context** – An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).
NTP authentication key numbers and values must match on both the server and client.

WEB INTERFACE

To add an entry to NTP authentication key list:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Add NTP Authentication Key from the Action list.
4. Enter the index number and MD5 authentication key string.
5. Click Apply.

Figure 18: Adding an NTP Authentication Key

The screenshot shows the 'System > Time' configuration page. The 'Step' dropdown is set to '2. Configure Time Server' and the 'Action' dropdown is set to 'Add NTP Authentication Key'. There are two input fields: 'Authentication Key (1-65535)' with the value '3' and 'Key Context (1-32)' with the value 'S1507N122103J068173M'. At the bottom right are 'Apply' and 'Revert' buttons.

To show the list of configured NTP authentication keys:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Show NTP Authentication Key from the Action list.

Figure 19: Showing the NTP Authentication Key List

The screenshot shows the 'System > Time' configuration page with the 'Action' dropdown set to 'Show NTP Authentication Key'. Below the dropdowns, it says 'NTP Authentication Key List Total: 1'. There is a table with two columns: 'Authentication Key' and 'Key Context'. The table contains one row with the values '3' and '8J0774Q6699747D10867F125505J62770084708278G1357878N8475052H3Q69137L8'. At the bottom right are 'Delete' and 'Revert' buttons.

Authentication Key	Key Context
3	8J0774Q6699747D10867F125505J62770084708278G1357878N8475052H3Q69137L8

SETTING THE TIME ZONE Use the System > Time (Configure Time Zone) page to set the time zone. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude, which passes through Greenwich, England. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is west (before) or east (after) of UTC. You can choose one of the 80 predefined time zone definitions, or you can manually configure the parameters for your local time zone.

CLI REFERENCES

- ◆ "clock timezone" on page 774

PARAMETERS

The following parameters are displayed:

- ◆ **Name** – Assigns a name to the time zone. (Range: 1-30 characters)
- ◆ **Hours** (-12-13) – The number of hours before or after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- ◆ **Minutes** (0-59) – The number of minutes before/after UTC.

WEB INTERFACE

To set your local time zone:

1. Click System, then Time.
2. Select Configure Time Zone from the Step list.
3. Set the offset for your time zone relative to the UTC in hours and minutes.
4. Click Apply.

Figure 20: Setting the Time Zone

The screenshot shows a web interface for configuring the system time zone. At the top, it says 'System > Time'. Below that is a 'Step:' dropdown menu currently showing '3. Configure Time Zone'. The main area contains three labeled input fields: 'Name' with the value 'UTC', 'Hours (-12-13)' with the value '0', and 'Minutes (0-59)' with the value '0'. At the bottom right of the form are two buttons: 'Apply' and 'Revert'.

CONFIGURING THE CONSOLE PORT

Use the System > Console menu to configure connection parameters for the switch's console port. You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial console port. Management access through the console port is controlled by various parameters, including a password (only configurable through the CLI), time outs, and basic communication settings. Note that these parameters can be configured via the web or CLI interface.

CLI REFERENCES

- ◆ ["Line" on page 746](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 10-300 seconds; Default: 300 seconds)
- ◆ **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 60-65535 seconds; Default: 600 seconds)
- ◆ **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 1-120; Default: 3 attempts)
- ◆ **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 1-65535 seconds; Default: Disabled)
- ◆ **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)
- ◆ **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)
- ◆ **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- ◆ **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud; Default: 115200 baud)



NOTE: The password for the console connection can only be configured through the CLI (see ["password" on page 750](#)).

NOTE: Password checking can be enabled or disabled for logging in to the console connection (see ["login" on page 749](#)). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port:

1. Click System, then Console.
2. Specify the connection parameters as required.
3. Click Apply

Figure 21: Console Port Settings

System > Console

Login Timeout (10-300)	<input type="text" value="300"/> sec
Exec Timeout (60-65535)	<input checked="" type="checkbox"/> <input type="text" value="600"/> sec
Password Threshold (1-120)	<input checked="" type="checkbox"/> <input type="text" value="3"/>
Silent Time (1-65535)	<input type="checkbox"/> <input type="text"/> sec
Data Bits	<input type="text" value="8"/>
Stop Bits	<input type="text" value="1"/>
Parity	<input type="text" value="None"/>
Speed	<input type="text" value="115200"/> baud

CONFIGURING TELNET SETTINGS

Use the System > Telnet menu to configure parameters for accessing the CLI over a Telnet connection. You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other parameters set, including the TCP port number, time outs, and a password. Note that the password is only configurable through the CLI.) These parameters can be configured via the web or CLI interface.

CLI REFERENCES

- ◆ ["Line" on page 746](#)
- ◆ ["Telnet Server" on page 850](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- ◆ **TCP Port** – Sets the TCP port number for Telnet on the switch. (Range: 1-65535; Default: 23)
- ◆ **Max Sessions** – Sets the maximum number of Telnet sessions that can simultaneously connect to this system. (Range: 0-8; Default: 8)
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).
- ◆ **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 10-300 seconds; Default: 300 seconds)
- ◆ **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 60-65535 seconds; Default: 600 seconds)
- ◆ **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 1-120; Default: 3 attempts)
- ◆ **Silent Time** – Sets the amount of time the management interface is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 1-65535 seconds; Default: Disabled)



NOTE: The password for the Telnet connection can only be configured through the CLI (see ["password" on page 750](#)).

NOTE: Password checking can be enabled or disabled for login to the console connection (see ["login" on page 749](#)). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port:

1. Click System, then Telnet.
2. Specify the connection parameters as required.
3. Click Apply

Figure 22: Telnet Connection Settings

DISPLAYING CPU UTILIZATION

Use the System > CPU Utilization page to display information on CPU utilization.

CLI REFERENCES

- ◆ ["show process cpu" on page 727](#)

PARAMETERS

The following parameters are displayed:

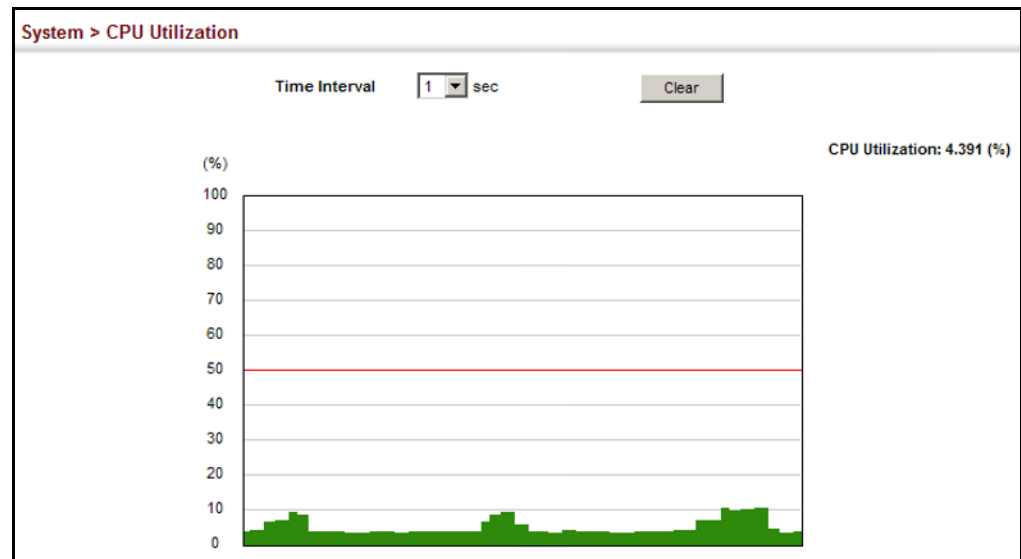
- ◆ **Time Interval** – The interval at which to update the displayed utilization rate. (Options: 1, 5, 10, 30, 60 seconds; Default: 1 second)
- ◆ **CPU Utilization** – CPU utilization over specified interval.

WEB INTERFACE

To display CPU utilization:

1. Click System, then CPU Utilization.
2. Change the update interval if required. Note that the interval is changed as soon as a new setting is selected.

Figure 23: Displaying CPU Utilization



DISPLAYING MEMORY UTILIZATION

Use the System > Memory Status page to display memory utilization parameters.

CLI REFERENCES

- ◆ ["show memory" on page 726](#)

PARAMETERS

The following parameters are displayed:

- ◆ **Free Size** – The amount of memory currently free for use.
- ◆ **Used Size** – The amount of memory allocated to active processes.
- ◆ **Total** – The total amount of system memory.

WEB INTERFACE

To display memory utilization:

1. Click System, then Memory Status.

Figure 24: Displaying Memory Utilization

System > Memory Status		
Memory Status		
Free Size	138,711,040 bytes	51%
Used Size	129,724,416 bytes	49%
Total	268,435,456 bytes	

RESETTING THE SYSTEM

Use the System > Reset menu to restart the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

CLI REFERENCES

- ◆ "reload (Privileged Exec)" on page 712
- ◆ "reload (Global Configuration)" on page 708
- ◆ "show reload" on page 713

COMMAND USAGE

- ◆ This command resets the entire system.
- ◆ 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 736](#)).

PARAMETERS

The following parameters are displayed:

System Reload Information

- ◆ **Reload Settings** – Displays information on the next scheduled reload and selected reload mode as shown in the following example:
 "The switch will be rebooted at March 9 12:00:00 2012. Remaining Time: 0 days, 2 hours, 46 minutes, 5 seconds.
 Reloading switch regularly time: 12:00 everyday."
- ◆ **Refresh** – Refreshes reload information. Changes made through the console or to system time may need to be refreshed to display the current settings.
- ◆ **Cancel** – Cancels the current settings shown in this field.

System Reload Configuration

- ◆ **Reset Mode** – Restarts the switch immediately or at the specified time(s).
 - **Immediately** – Restarts the system immediately.
 - **In** – Specifies an interval after which to reload the switch. (The specified time must be equal to or less than 24 days.)
 - *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)
 - **At** – Specifies a time at which to reload the switch.
 - DD - The day of the month at which to reload. (Range: 1-31)
 - MM - The month at which to reload. (Range: 01-12)
 - YYYY - The year at which to reload. (Range: 2001-2050)
 - HH - The hour at which to reload. (Range: 0-23)
 - MM - The minute at which to reload. (Range: 0-59)
 - **Regularly** – Specifies a periodic interval at which to reload the switch.

Time

- HH - The hour at which to reload. (Range: 0-23)
- MM - The minute at which to reload. (Range: 0-59)

Period

- Daily - Every day.
- Weekly - Day of the week at which to reload. (Range: Sunday ... Saturday)
- Monthly - Day of the month at which to reload. (Range: 1-31)

Save Current Settings

- ◆ **Save** – Click this button to save the current configuration settings.

Use Factory Default Settings and Reboot

- ◆ **Factory Default Settings & Reboot** – Click this button to restore the factory default settings and reboot the system.

WEB INTERFACE

To restart the switch:

1. Click System, then Reset.
2. Select the required reset mode.
3. For any option other than to reset immediately, fill in the required parameters
4. Click Apply.
5. When prompted, confirm that you want reset the switch.

Figure 25: Restarting the Switch (Immediately)

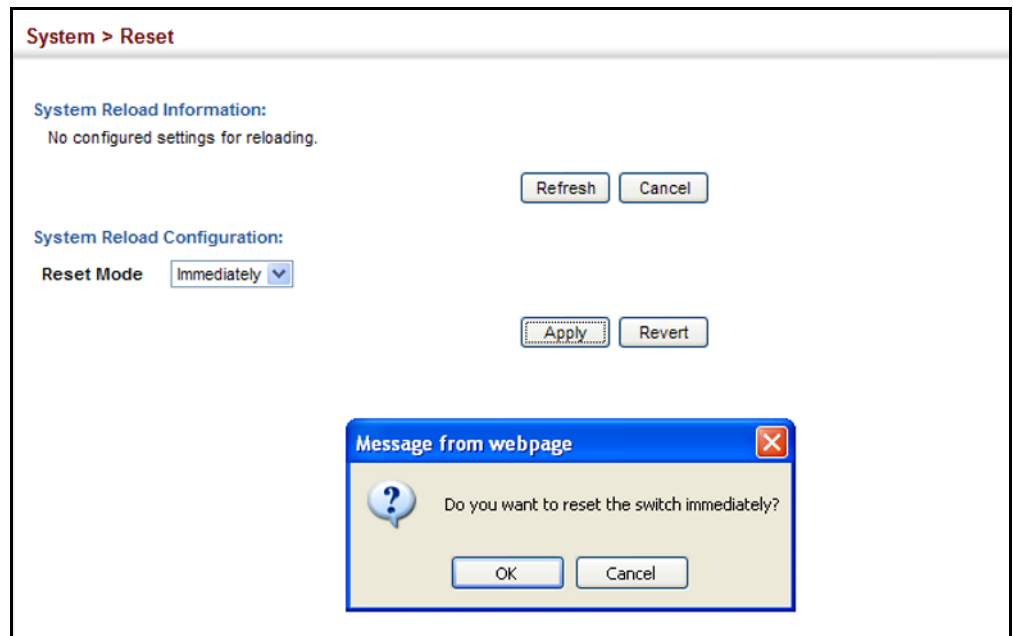


Figure 26: Restarting the Switch (In)

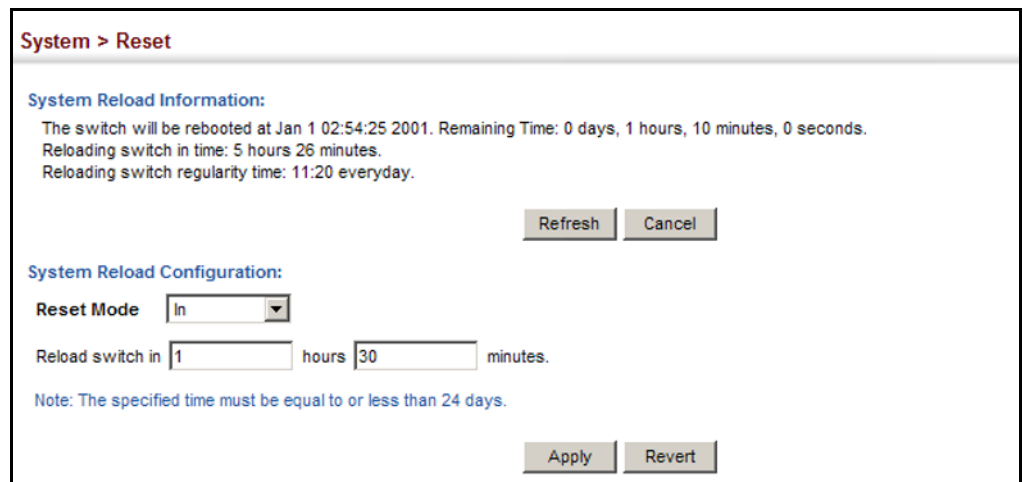


Figure 27: Restarting the Switch (At)

System > Reset

System Reload Information:
The switch will be rebooted at Jan 1 02:54:25 2001. Remaining Time: 0 days, 1 hours, 10 minutes, 0 seconds.
Reloading switch in time: 5 hours 26 minutes.
Reloading switch regularity time: 11:20 everyday.

RefreshCancel

System Reload Configuration:
Reset Mode At
Reload switch at 19/10/2009 (DD/MM/YYYY) 05:00 (HH:MM)
Warning: You have to setup system time first.Otherwise this function won't work.

ApplyRevert

Figure 28: Restarting the Switch (Regularly)

System > Reset

System Reload Information:
No configured settings for reloading.

RefreshCancel

System Reload Configuration:
Reset Mode Regularly
Time 05:30 (HH:MM)
Period ☒ Daily
☐ Weekly Sunday
☐ Monthly 1
Warning: You have to setup system time first.Otherwise this function won't work.

ApplyRevert

This chapter describes the following topics:

- ◆ [Port Configuration](#) – Configures connection settings, including auto-negotiation, or manual setting of speed, duplex mode, and flow control.
- ◆ [Local Port Mirroring](#) – Sets the source and target ports for mirroring on the local switch.
- ◆ [Remote Port Mirroring](#) – Configures mirroring of traffic from remote switches for analysis at a destination port on the local switch.
- ◆ [Displaying Statistics](#) – Shows Interface, Etherlike, and RMON port statistics in table or chart form.
- ◆ [Cable Test](#) – Performs cable diagnostics on the specified port.
- ◆ [Trunk Configuration](#) – Configures static or dynamic trunks.
- ◆ [Saving Power](#) – Adjusts the power provided to ports based on the length of the cable used to connect to other devices.
- ◆ [Flow Sampling](#) – Configures periodic sampling of traffic flows.
- ◆ [Traffic Segmentation](#) – Configures the uplinks and down links to a segmented group of ports.
- ◆ [VLAN Trunking](#) – Configures a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

PORT CONFIGURATION

This section describes how to configure port connections, mirror traffic from one port to another, and run cable diagnostics.

CONFIGURING BY PORT LIST

Use the Interface > Port > General (Configure by Port List) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

CLI REFERENCES

- ◆ ["Interface Commands" on page 973](#)

COMMAND USAGE

- ◆ Auto-negotiation must be disabled before you can configure or force a Gigabit RJ-45 interface to use the Speed/Duplex mode or Flow Control options.
- ◆ When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.
- ◆ 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.
- ◆ The Speed/Duplex mode is fixed at 1000full on 1000BASE SFP ports¹ and 10Gfull on the 10GBASE SFP+ ports. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Type** – Indicates the port type. (1000BASE-T, 1000BASE SFP¹, 10GBASE SFP+)
- ◆ **Name** – Allows you to label an interface. (Range: 1-64 characters)
- ◆ **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons. (Default: Enabled)
- ◆ **Media Type** – Configures the forced/preferred port type to use for combination ports. (Only applies to ports 23-24 on ECS4510-28F.)
 - **Copper-Forced** - Always uses the RJ-45 port.
 - **SFP-Forced 1000SFP** - Always uses the SFP port at 1000 Mbps, Full Duplex.
 - **SFP-Forced 100FX** - Always uses the SFP port at 100 Mbps, Full Duplex.
 - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. The speed is set by autonegotiation, and the mode is fixed at Full Duplex. (This is the default setting.)

1. ECS4510-28F

- ◆ **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.
 - **10h** - Supports 10 Mbps half-duplex operation.
 - **10f** - Supports 10 Mbps full-duplex operation.
 - **100h** - Supports 100 Mbps half-duplex operation.
 - **100f** - Supports 100 Mbps full-duplex operation.
 - **1000h** - Not supported.
 - **1000f** (Gigabit ports only) - Supports 1000 Mbps full-duplex operation.
 - **10Gh** - Not supported.
 - **10Gf** (10 Gigabit ports only) - Supports 10 Gbps full-duplex operation.
 - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames.
 - **FC** - 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 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.

Default: Autonegotiation enabled on Gigabit and 10 Gigabit ports;
Advertised capabilities for

 - 100BASE-FX (SFP² / SFP+) – 100full
 - 1000BASE-T – 10half, 10full, 100half, 100full, 1000full
 - 1000BASE-SX/LX/ZX (SFP² / SFP+) – 1000full
 - 10GBASE-SR/LR/ER (SFP+) – 10Gfull
- ◆ **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
- ◆ **Flow Control** – Allows automatic or manual selection of flow control.

WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port List from the Action List.
3. Modify the required interface settings.

2. ECS4510-28F

4. Click Apply.

Figure 29: Configuring Connections by Port List

Interface > Port > General

Action: Configure by Port List

Port List Total: 28

Port	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control
1	1000BASE-T		<input checked="" type="checkbox"/> Enabled	None	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> 10Gh <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input checked="" type="checkbox"/> 1000f <input type="checkbox"/> 10Gf <input type="checkbox"/> FC	100full	<input checked="" type="checkbox"/> Enabled
2	1000BASE-T		<input checked="" type="checkbox"/> Enabled	None	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> 10Gh <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input checked="" type="checkbox"/> 1000f <input type="checkbox"/> 10Gf <input type="checkbox"/> FC	100full	<input checked="" type="checkbox"/> Enabled
3	1000BASE-T		<input checked="" type="checkbox"/> Enabled	None	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> 10Gh <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input checked="" type="checkbox"/> 1000f <input type="checkbox"/> 10Gf <input type="checkbox"/> FC	100full	<input checked="" type="checkbox"/> Enabled

CONFIGURING BY PORT RANGE

Use the Interface > Port > General (Configure by Port Range) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

For more information on command usage and a description of the parameters, refer to ["Configuring by Port List" on page 151](#).

CLI REFERENCES

- ◆ ["Interface Commands" on page 973](#)

WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port Range from the Action List.
3. Enter to range of ports to which your configuration changes apply.
4. Modify the required interface settings.
5. Click Apply.

Figure 30: Configuring Connections by Port Range

Interface > Port > General

Action: Configure by Port Range

Port Range (1-28) 1 - 5

Admin ☒ Enabled

Autonegotiation ☒ Enabled

☐ 10h ☒ 100h ☐ 1000h ☐ 10Gh ☐ Sym

☒ 10f ☐ 100f ☒ 1000f ☐ 10Gf ☐ FC

Speed Duplex 10half

Flow Control ☒ Enabled

Apply Revert

DISPLAYING CONNECTION STATUS Use the Interface > Port > General (Show Information) page to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

CLI REFERENCES

- ◆ ["show interfaces status" on page 985](#)

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier.
- ◆ **Type** – Indicates the port type. (1000BASE-T, 1000BASE SFP³, 10GBASE SFP+)
- ◆ **Name** – Interface label.
- ◆ **Admin** – Shows if the port is enabled or disabled.
- ◆ **Oper Status** – Indicates if the link is Up or Down.
- ◆ **Media Type** – Only applies to ports 23-24 on ECS4510-28F.
- ◆ **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- ◆ **Oper Speed Duplex** – Shows the current speed and duplex mode.
- ◆ **Oper Flow Control** – Shows the flow control type used.

3. ECS4510-28F

WEB INTERFACE

To display port connection parameters:

1. Click Interface, Port, General.
2. Select Show Information from the Action List.

Figure 31: Displaying Port Information

Interface > Port > General

Action: Show Information

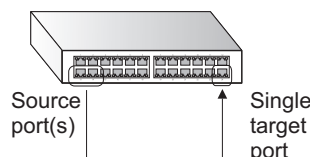
Port List Total: 28

Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	1000BASE-T		Enabled	Up	None	Enabled	100full	None
2	1000BASE-T		Enabled	Up	None	Enabled	1000full	None
3	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
4	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
5	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
6	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
7	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
8	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
9	1000BASE-T		Enabled	Down	None	Enabled	1000full	None
10	1000BASE-T		Enabled	Down	None	Enabled	1000full	None

CONFIGURING LOCAL PORT MIRRORING

Use the Interface > Port > Mirror page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Figure 32: Configuring Local Port Mirroring



CLI REFERENCES

- ◆ ["Local Port Mirroring Commands" on page 1013](#)

COMMAND USAGE

- ◆ Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in this section), or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in ["Configuring Remote Port Mirroring" on page 158](#)).
- ◆ Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- ◆ When mirroring VLAN traffic (see ["Configuring VLAN Mirroring" on page 223](#)) or packets based on a source MAC address (see ["Configuring](#)

MAC Address Mirroring" on page 232), the target port cannot be set to the same target ports as that used for port mirroring by this command.

- ◆ When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.
- ◆ The destination port cannot be a trunk or trunk member port.
- ◆ Note that Spanning Tree BPDU packets are not mirrored to the target port.

PARAMETERS

These parameters are displayed:

- ◆ **Source Port** – The port whose traffic will be monitored.
- ◆ **Target Port** – The port that will mirror the traffic on the source port.
- ◆ **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Both)

WEB INTERFACE

To configure a local mirror session:

1. Click Interface, Port, Mirror.
2. Select Add from the Action List.
3. Specify the source port.
4. Specify the monitor port.
5. Specify the traffic type to be mirrored.
6. Click Apply.

Figure 33: Configuring Local Port Mirroring

Interface > Port > Mirror

Action:

Source Port Unit Port

Target Port Unit Port

Type

To display the configured mirror sessions:

1. Click Interface, Port, Mirror.
2. Select Show from the Action List.

Figure 34: Displaying Local Port Mirror Sessions

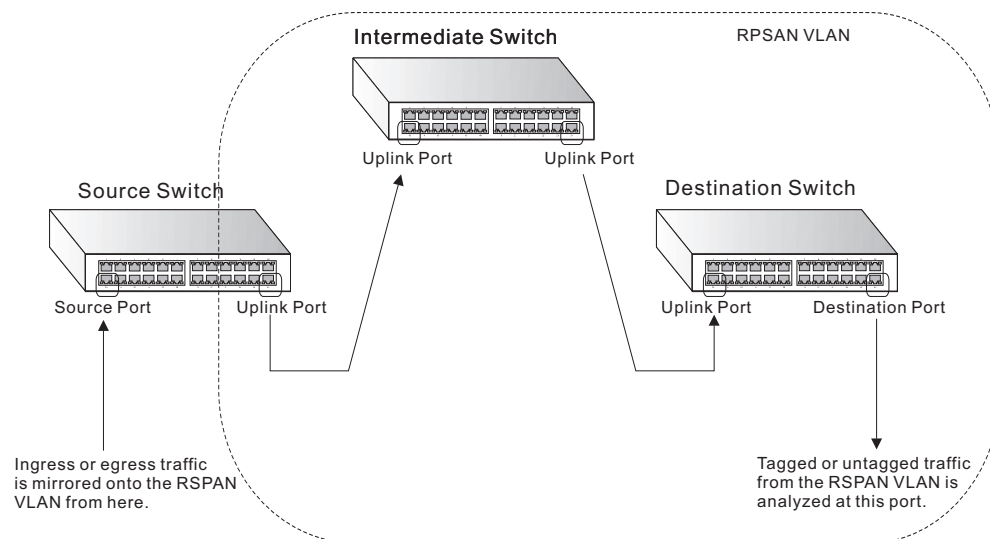
Interface > Port > Mirror			
Action: Show			
Mirror Session List Total: 2			
	Source (Unit/Port)	Target (Unit/Port)	Type
<input type="checkbox"/>	1 / 7	1 / 8	Both
<input type="checkbox"/>	1 / 9	1 / 10	Rx

Delete Revert

CONFIGURING REMOTE PORT MIRRORING

Use the Interface > RSPAN page to mirror traffic from remote switches for analysis at a destination port on the local switch. This feature, also called Remote Switched Port Analyzer (RSPAN), carries traffic generated on the specified source ports for each session over a user-specified VLAN dedicated to that RSPAN session in all participating switches. Monitored traffic from one or more sources is copied onto the RSPAN VLAN through IEEE 802.1Q trunk or hybrid ports that carry it to any RSPAN destination port monitoring the RSPAN VLAN as shown in the figure below.

Figure 35: Configuring Remote Port Mirroring



CLI REFERENCES

- ◆ ["RSPAN Mirroring Commands" on page 1016](#)

COMMAND USAGE

- ◆ Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in ["Configuring Local Port Mirroring" on page 156](#)), or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in this section).

- ◆ *Configuration Guidelines*

Take the following step to configure an RSPAN session:

1. Use the VLAN Static List (see ["Configuring VLAN Groups" on page 196](#)) to reserve a VLAN for use by RSPAN (marking the "Remote VLAN" field on this page. (Default VLAN 1 is prohibited.)
2. Set up the source switch on the RSPAN configuration page by specifying the mirror session, the switch's role (Source), the RSPAN VLAN, and the uplink port⁴. Then specify the source port(s), and the traffic type to monitor (Rx, Tx or Both).
3. Set up all intermediate switches on the RSPAN configuration page, entering the mirror session, the switch's role (Intermediate), the RSPAN VLAN, and the uplink port(s).
4. Set up the destination switch on the RSPAN configuration page by specifying the mirror session, the switch's role (Destination), the destination port⁴, whether or not the traffic exiting this port will be tagged or untagged, and the RSPAN VLAN. Then specify each uplink port where the mirrored traffic is being received.

- ◆ *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.
- *Local/Remote Mirror* – The destination of a local mirror session (created on the Interface > Port > Mirror page) 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.

4. Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink or destination ports – access ports are not allowed (see ["Adding Static Members to VLANs" on page 199](#)).

- *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.
- *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.

PARAMETERS

These parameters are displayed:

- ◆ **Session** – A number identifying this RSPAN session. (Range: 1)
Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled (see [page 156](#)), then no session can be configured for RSPAN.
- ◆ **Operation Status** – Indicates whether or not RSPAN is currently functioning.
- ◆ **Switch Role** – Specifies the role this switch performs in mirroring traffic.
 - **None** – This switch will not participate in RSPAN.
 - **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.
- ◆ **Remote VLAN** – The VLAN to which traffic mirrored from the source port will be flooded. The VLAN specified in this field must first be reserved for the RSPAN application using the VLAN > Static page (see [page 196](#)).
- ◆ **Uplink Port** – A port on any switch participating in RSPAN through which mirrored traffic is passed on to or received from the RSPAN VLAN.

Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports⁴ configured on an intermediate or destination switch.

Only destination and uplink ports will be assigned by the switch as members of the RSPAN VLAN. Ports cannot be manually assigned to an RSPAN VLAN through the VLAN > Static page. Nor can GVRP

dynamically add port members to an RSPAN VLAN. Also, note that the VLAN > Static (Show) page will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

- ◆ **Type** – Specifies the traffic type to be mirrored remotely. (Options: Rx, Tx, Both)
- ◆ **Destination Port** – Specifies the destination port⁴ to monitor the traffic mirrored from the source ports. 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. Also note that a destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.
- ◆ **Tag** – Specifies whether or not the traffic exiting the destination port to the monitoring device carries the RSPAN VLAN tag.

WEB INTERFACE

To configure a remote mirror session:

1. Click Interface, RSPAN.
2. Set the Switch Role to None, Source, Intermediate, or Destination.
3. Configure the required settings for each switch participating in the RSPAN VLAN.
4. Click Apply.

Figure 36: Configuring Remote Port Mirroring (Source)

Interface > RSPAN

Session1

Operation StatusUp

Switch RoleSource

Remote VLAN2

Uplink Port4

Source Port Configuration List Total: 28

Source Port	Type
1	Rx
2	Rx
3	None
4	None
5	Tx

Figure 37: Configuring Remote Port Mirroring (Intermediate)

Interface > RSPAN

Session: 1

Operation Status: Up

Switch Role: Intermediate

Remote VLAN: 2

Uplink Port List Total: 28

Port	Uplink
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input type="checkbox"/>

Figure 38: Configuring Remote Port Mirroring (Destination)

Interface > RSPAN

Session: 1

Operation Status: Up

Switch Role: Destination

Destination Port: 1

Tag: Untagged

Remote VLAN: 2

Uplink Port List Total: 28

Port	Uplink
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input type="checkbox"/>

SHOWING PORT OR TRUNK STATISTICS

Use the Interface > Port/Trunk > Statistics or Chart page to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.



NOTE: RMON groups 2, 3 and 9 can only be accessed using SNMP management software.

CLI REFERENCES

- ◆ ["show interfaces counters" on page 983](#)

PARAMETERS

These parameters are displayed:

Table 7: Port Statistics

Parameter	Description
<i>Interface Statistics</i>	
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Transmitted Unicast Packets	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.
Received Discarded Packets	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.
Transmitted Discarded Packets	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.
Received Multicast Packets	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.
Transmitted Multicast Packets	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.
Received Broadcast Packets	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.
Transmitted Broadcast Packets	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.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
<i>Etherlike Statistics</i>	
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.
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.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.

Table 7: Port Statistics (Continued)

Parameter	Description
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Alignment Errors	The number of alignment errors (missynchronized data packets).
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.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
<i>RMON Statistics</i>	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
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.
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.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received 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.
64 Bytes Packets	The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Packets	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 Byte Packets	
256-511 Byte Packets	
512-1023 Byte Packets	
1024-1518 Byte Packets	
1519-1536 Byte Packets	

Table 7: Port Statistics (Continued)

Parameter	Description
<i>Utilization Statistics</i>	
Input Octets in kbits per second	Number of octets entering this interface in kbits/second.
Input Packets per second	Number of packets entering this interface per second.
Input Utilization	The input utilization rate for this interface.
Output Octets in kbits per second	Number of octets leaving this interface in kbits/second.
Output Packets per second	Number of packets leaving this interface per second.
Output Utilization	The output utilization rate for this interface.

WEB INTERFACE

To show a list of port statistics:

1. Click Interface, Port, Statistics.
2. Select the statistics mode to display (Interface, Etherlike, RMON or Utilization).
3. Select a port from the drop-down list.
4. Use the Refresh button at the bottom of the page if you need to update the screen.

Figure 39: Showing Port Statistics (Table)

Interface > Port > Statistics

Mode ☒ Interface ☐ Etherlike ☐ RMON ☐ Utilization

Port

1

☐ Auto-refresh

Interface Statistics

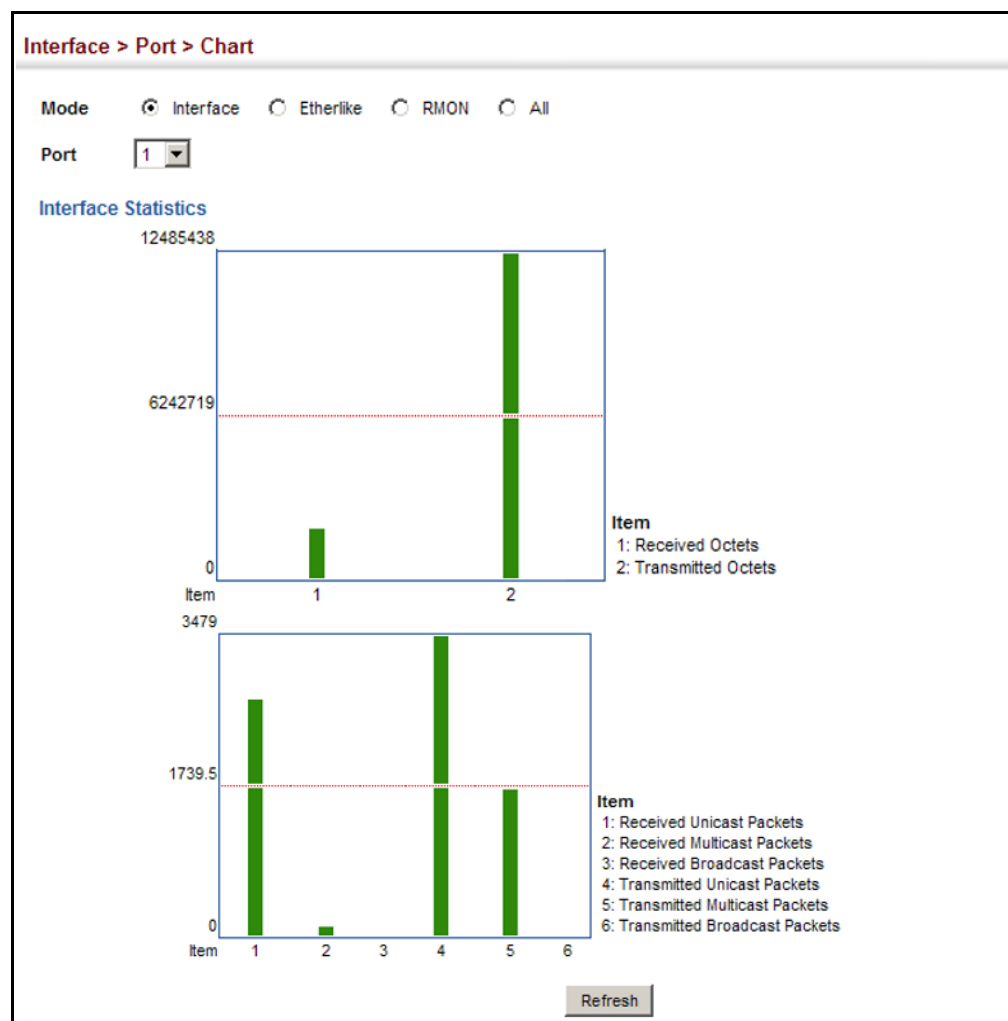
Received Octets	1087697	Transmitted Octets	5274231
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	5342	Transmitted Unicast Packets	6891
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	3692	Transmitted Multicast Packets	3940
Received Broadcast Packets	145	Transmitted Broadcast Packets	2
Received Unknown Packets	0		

Refresh

To show a chart of port statistics:

1. Click Interface, Port, Chart.
2. Select the statistics mode to display (Interface, Etherlike, RMON or All).
3. If Interface, Etherlike, RMON statistics mode is chosen, select a port from the drop-down list. If All (ports) statistics mode is chosen, select the statistics type to display.

Figure 40: Showing Port Statistics (Chart)



PERFORMING CABLE DIAGNOSTICS

Use the Interface > Port > Cable Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

CLI REFERENCES

- ◆ ["Interface Commands" on page 973](#)

COMMAND USAGE

- ◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test methods. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- ◆ Cable diagnostics can only be performed on twisted-pair media.
- ◆ This cable test is only accurate for cables 7 - 140 meters long.
- ◆ The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.
- ◆ Potential conditions which may be listed by the diagnostics include:
 - OK: Correctly terminated pair
 - Open: Open pair, no link partner
 - Short: Shorted pair
 - Not Supported: This message is displayed for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps, or for any 10G Ethernet ports.
 - Impedance mismatch: Terminating impedance is not in the reference range.
- ◆ Ports are linked down while running cable diagnostics.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Switch port identifier.
- ◆ **Type** – Displays media type. (GE – Gigabit Ethernet, Other – SFP¹ / SFP+)
- ◆ **Link Status** – Shows if the port link is up or down.
- ◆ **Test Result** – 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.

To ensure more accurate measurement of the length to a fault, first disable power-saving mode on the link partner before running cable diagnostics.

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.
- ◆ **Last Updated** – Shows the last time this port was tested.

WEB INTERFACE

To test the cable attached to a port:

1. Click Interface, Port, Cable Test.
2. Click Test for any port to start the cable test.

Figure 41: Performing Cable Tests

Port	Type	Link Status	Test Result (Cable/Fault Distance in Meters)		Last Updated	Action
			Pair A (meters)	Pair B (meters)		
21	GE	Down	Not Tested	Not Tested		<button>Test</button>
22	GE	Down	Not Tested	Not Tested		<button>Test</button>
23	GE	Down	No Cable (0)	No Cable (0)	2012-03-09 07:45:29	<button>Test</button>
24	GE	Up	Not Supported	Not Supported	2012-03-09 07:44:59	<button>Test</button>
25	Other	Down	Testing...	Testing...		<button>Test</button>
26	Other	Down	Not Tested	Not Tested		<button>Test</button>
27	GE	Down	Not Tested	Not Tested		<button>Test</button>
28	GE	Down	Not Tested	Not Tested		<button>Test</button>

Note: After every test action, wait several seconds and click the refresh button to display test results.

Refresh

TRUNK CONFIGURATION

This section describes how to configure static and dynamic trunks.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 5 trunks at a time on the switch.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

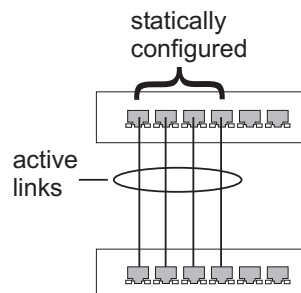
COMMAND USAGE

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- ◆ Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- ◆ You can create up to 16 trunks on a switch, with up to eight ports per trunk.
- ◆ The ports at both ends of a connection must be configured as trunk ports.
- ◆ When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- ◆ The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), 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.
- ◆ STP, VLAN, and IGMP settings can only be made for the entire trunk.

CONFIGURING A STATIC TRUNK Use the Interface > Trunk > Static page to create a trunk, assign member ports, and configure the connection parameters.

Figure 42: Configuring Static Trunks



CLI REFERENCES

- ◆ ["Link Aggregation Commands" on page 993](#)
- ◆ ["Interface Commands" on page 973](#)

COMMAND USAGE

- ◆ When configuring static trunks, you may not be able to link switches of different types, depending on the vendor's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- ◆ To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

PARAMETERS

These parameters are displayed:

- ◆ **Trunk ID** – Trunk identifier. (Range: 1-16)
- ◆ **Member** – The initial trunk member. Use the Add Member page to configure additional members.
 - **Unit** – Unit identifier. (Range: 1)
 - **Port** – Port identifier. (Range: 1-28/52)

WEB INTERFACE

To create a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure Trunk from the Step list.
3. Select Add from the Action list.
4. Enter a trunk identifier.
5. Set the unit and port for the initial trunk member.
6. Click Apply.

Figure 43: Creating Static Trunks

The screenshot shows a web interface for configuring static trunks. At the top, the breadcrumb navigation reads "Interface > Trunk > Static". Below this, there are two dropdown menus: "Step:" with "1. Configure Trunk" selected, and "Action:" with "Add" selected. The main configuration area contains a "Trunk ID (1-16)" label followed by a text input field containing the number "1". Below this is a "Member" label, followed by "Unit" and "Port" labels, each with a dropdown menu. The "Unit" dropdown shows "1" and the "Port" dropdown shows "1". At the bottom right of the form are two buttons: "Apply" and "Revert".

To add member ports to a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure Trunk from the Step list.
3. Select Add Member from the Action list.
4. Select a trunk identifier.
5. Set the unit and port for an additional trunk member.
6. Click Apply.

Figure 44: Adding Static Trunks Members

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add Member

Trunk 1

Member Unit 1 Port 1

Apply Revert

To configure connection parameters for a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Configure from the Action list.
4. Modify the required interface settings. (Refer to ["Configuring by Port List" on page 151](#) for a description of the parameters.)
5. Click Apply.

Figure 45: Configuring Connection Parameters for a Static Trunk

Interface > Trunk > Static

Step: 2. Configure General Action: Configure

Static Trunk List Total: 1

Trunk	Type	Name	Admin	Autonegotiation	Speed Duplex	Flow Control
1	1000BASE-T		Enabled	Enabled 10h 100h 1000h 10Gh 10f 100f 1000f 10Gf Sym FC	100full	Enabled

Apply Revert

To display trunk connection parameters:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Show Information from the Action list.

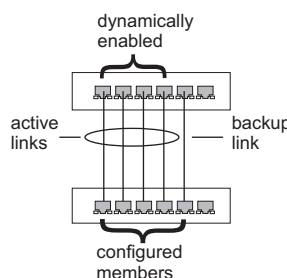
Figure 46: Showing Information for Static Trunks

Trunk	Type	Name	Admin	Oper Status	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	1000BASE-T		Enabled	Down	Enabled	1000full	None

CONFIGURING A DYNAMIC TRUNK

Use the Interface > Trunk > Dynamic pages to set the administrative key for an aggregation group, enable LACP on a port, configure protocol parameters for local and partner ports, or to set Ethernet connection parameters.

Figure 47: Configuring Dynamic Trunks



CLI REFERENCES

- ◆ ["Link Aggregation Commands" on page 993](#)

COMMAND USAGE

- ◆ To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- ◆ If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- ◆ A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- ◆ 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.

- ◆ All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- ◆ Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.



NOTE: If the LACP admin key is not set when a channel group is formed (i.e., it has a null value of 0), the operational value of this key is set to the same value as the port admin key used by the interfaces that joined the group (see the [show lacp internal](#) command described on [page 1002](#)).

PARAMETERS

These parameters are displayed:

Configure Aggregator

- ◆ **Admin Key** – LACP administration key is used to identify a specific link aggregation group (LAG) during local LACP setup on the switch. (Range: 0-65535)
- ◆ **Timeout Mode** – The timeout to wait for the next LACP data unit (LACPDU):
 - **Long Timeout** – Specifies a slow timeout of 90 seconds. (This is the default setting.)
 - **Short Timeout** – Specifies a fast timeout of 3 seconds.

The timeout is set in the LACP timeout bit of the Actor State field in transmitted LACPDUs. 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.

Configure Aggregation Port - General

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **LACP Status** – Enables or disables LACP on a port.

Configure Aggregation Port - Actor/Partner

- ◆ **Port** – Port number. (Range: 1-28/52)
- ◆ **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default – Actor: 1, Partner: 0)

By default, the Actor Admin Key is determined by port's link speed, and copied to Oper Key. The Partner Admin Key is assigned to zero, and the Oper Key is set based upon LACP PDUs received from the Partner.
- ◆ **System Priority** – LACP system 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: 32768)

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.
- ◆ **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)
 - 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.



NOTE: Configuring LACP settings for a port only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with that port.

NOTE: Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

WEB INTERFACE

To configure the admin key for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregator from the Step list.
3. Set the Admin Key and timeout mode for the required LACP group.
4. Click Apply.

Figure 48: Configuring the LACP Aggregator Admin Key

Interface > Trunk > Dynamic

Step: 1. Configure Aggregator

Trunk List Total: 16

Trunk	Admin Key (0-65535)	Timeout Mode
1	0	Long Timeout
2	0	Long Timeout
3	0	Long Timeout
4	0	Long Timeout
5	0	Long Timeout

To enable LACP for a port:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click General.
5. Enable LACP on the required ports.
6. Click Apply.

Figure 49: Enabling LACP on a Port

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

☒ General ☐ Actor ☐ Partner

Port List Total: 28

Port	LACP Status
1	<input type="checkbox"/> Enabled
2	<input checked="" type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled

To configure LACP parameters for group members:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click Actor or Partner.
5. Configure the required settings.
6. Click Apply.

Figure 50: Configuring LACP Parameters on a Port

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

☐ General ☒ Actor ☐ Partner

Port List Total: 28

Port	Admin Key (0-65535)	System Priority (0-65535)	Port Priority (0-65535)
1	3	32768	32768
2	3	32768	32768
3	1	32768	32768
4	1	32768	32768
5	1	32768	32768

To show the active members of a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Show Member from the Action List.
4. Select a Trunk.

Figure 51: Showing Members of a Dynamic Trunk

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show Member

Trunk 1

Member List Total: 2

Member (Unit/Port)
1/1
1/2

To configure connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Configure from the Action List.
4. Modify the required interface settings. (See ["Configuring by Port List" on page 151](#) for a description of the interface settings.)
5. Click Apply.

Figure 52: Configuring Connection Settings for Dynamic Trunks

Trunk	Type	Name	Admin	Autonegotiation	Speed Duplex	Flow Control
1	1000BASE-T		<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> 10Gh <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input checked="" type="checkbox"/> 1000f <input type="checkbox"/> 10Gf <input type="checkbox"/> Sym <input type="checkbox"/> FC	100full	<input checked="" type="checkbox"/> Enabled

Apply Revert

To display connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Show from the Action List.

Figure 53: Displaying Connection Parameters for Dynamic Trunks

Trunk	Type	Name	Admin	Oper Status	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	1000BASE-T		Enabled	Up	Enabled	1000full	None

DISPLAYING LACP PORT COUNTERS Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Counters) page to display statistics for LACP protocol messages.

CLI REFERENCES

◆ ["show lacp" on page 1002](#)

PARAMETERS

These parameters are displayed:

Table 8: LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	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.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

WEB INTERFACE

To display LACP port counters:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Counters.
5. Select a group member from the Port list.

Figure 54: Displaying LACP Port Counters

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

☒ Counters ☐ Internal ☐ Neighbors

Port 1

Trunk ID 2

Port Counters Information

LACPDUs Sent	29	LACPDUs Received	25
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

Refresh

DISPLAYING LACP
SETTINGS AND STATUS
FOR THE LOCAL SIDE

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Internal) page to display the configuration settings and operational state for the local side of a link aggregation.

CLI REFERENCES

◆ ["show lacp" on page 1002](#)

PARAMETERS

These parameters are displayed:

Table 9: LACP Internal Configuration Information

Parameter	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.
LACPDUs Interval	Number of seconds before invalidating received LACPDU information.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: <ul style="list-style-type: none">◆ Expired – The actor's receive machine is in the expired state;◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner.◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information.◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information.◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.

Table 9: LACP Internal Configuration Information (Continued)

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

WEB INTERFACE

To display LACP settings and status for the local side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Internal.
5. Select a group member from the Port list.

Figure 55: Displaying LACP Port Internal Information

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

☐ Counters
 ☒ Internal
 ☐ Neighbors

Port 1

Trunk ID 2

Port Internal Information

LACP System Priority	32768
LACP Port Priority	32768
Admin Key	3
Oper Key	3
LACPDUs Interval	30 sec
Admin State	Defaulted, Aggregation, Long timeout, LACP-activity
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

**DISPLAYING LACP
SETTINGS AND STATUS
FOR THE REMOTE SIDE**

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Neighbors) page to display the configuration settings and operational state for the remote side of a link aggregation.

CLI REFERENCES

- ◆ ["show lacp" on page 1002](#)

PARAMETERS

These parameters are displayed:

Table 10: LACP Remote Device Configuration Information

Parameter	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

WEB INTERFACE

To display LACP settings and status for the remote side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Neighbors.
5. Select a group member from the Port list.

Figure 56: Displaying LACP Port Remote Information

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port
Action: Show Information

☐ Counters
☐ Internal
☒ Neighbors

Port 3

Trunk ID 2

Port Neighbors Information

Partner Admin System ID	32768, 00-00-00-00-00-00
Partner Oper System ID	32768, 00-12-CF-61-24-2F
Partner Admin Port Number	3
Partner Oper Port Number	3
Port Admin Priority	32768
Port Oper Priority	32768
Admin Key	0
Oper Key	3
Admin State	Defaulted, Distributing, Collecting, Synchronization, Long timeout
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

SAVING POWER

Use the Interface > Green Ethernet page to enable power savings mode on the selected port.

CLI REFERENCES

- ◆ ["power-save" on page 990](#)
- ◆ ["show power-save" on page 991](#)

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.
- ◆ 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 (enters 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 when 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.

PARAMETERS

These parameters are displayed:

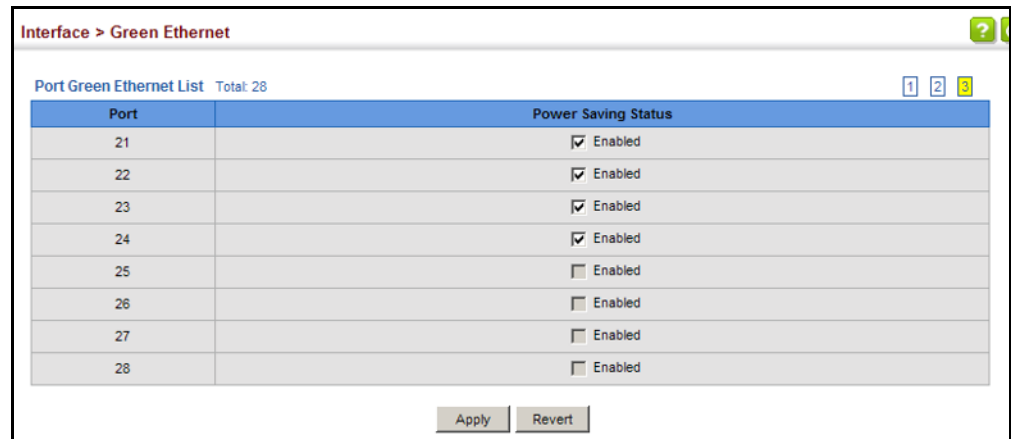
- ◆ **Port** – Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- ◆ **Power Saving Status** – Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements. (Default: Enabled on Gigabit Ethernet RJ-45 ports)

WEB INTERFACE

To enable power savings:

1. Click Interface, Green Ethernet.
2. Mark the Enabled check box for a port.
3. Click Apply.

Figure 57: Enabling Power Savings



Port	Power Saving Status
21	<input checked="" type="checkbox"/> Enabled
22	<input checked="" type="checkbox"/> Enabled
23	<input checked="" type="checkbox"/> Enabled
24	<input checked="" type="checkbox"/> Enabled
25	<input type="checkbox"/> Enabled
26	<input type="checkbox"/> Enabled
27	<input type="checkbox"/> Enabled
28	<input type="checkbox"/> Enabled

Apply Revert

SAMPLING TRAFFIC FLOWS

The flow sampling (sFlow) feature embedded on this switch, together with a remote sFlow Collector, can provide network administrators with an accurate, detailed and real-time overview of the types and levels of traffic present on their 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 will 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. The wire-speed transmission characteristic of the switch is thus preserved even at high traffic levels.

As the Collector receives streams from the various sFlow agents (other switches or routers) throughout the network, a timely, network-wide picture of utilization and traffic flows is created. Analysis of the sFlow stream(s) can reveal trends and information that can be leveraged in the following ways:

- ◆ Detecting, diagnosing, and fixing network problems
- ◆ Real-time congestion management
- ◆ Understanding application mix (P2P, Web, DNS, etc.) and changes
- ◆ Identification and tracing of unauthorized network activity
- ◆ Usage accounting
- ◆ Trending and capacity planning

CONFIGURING SFlow GLOBAL SETTINGS Use the Interface > sFlow (Configure Global) page to enable sFlow globally for the switch.

CLI REFERENCES

◆ "sflow" on page 815

PARAMETERS

These parameters are displayed in the web interface:

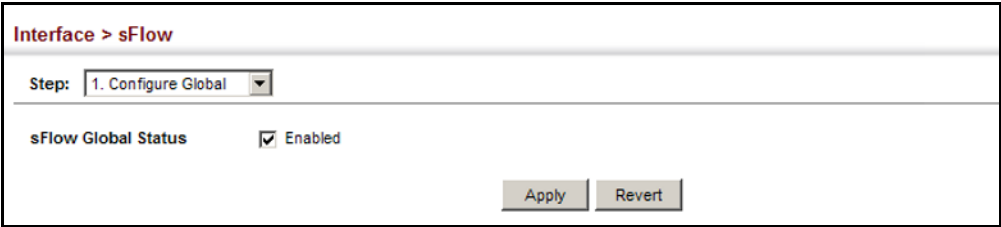
◆ **sFlow Global Status** – Enables sFlow globally for the switch.
(Default: Disabled)

WEB INTERFACE

To configure flow sampling:

1. Click Interface, sFlow.
2. Select Configure Global from the Step list.
3. Enable or disable flow sampling.
4. Click Apply.

Figure 58: Enabling Traffic Flow Sampling



CONFIGURING SFlow INTERFACE SETTINGS Use the Interface > sFlow (Configure Interface) page to set the source and destination parameters for the sampled data, payload parameters, and sampling interval.

CLI REFERENCES

◆ "Flow Sampling Commands" on page 815

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Port** – Choose the port to configure. (Range: 1-28/52; Default: 1)
- ◆ **Source Status** – Enables sFlow on the selected port.
- ◆ **Receiver Owner**⁵ – The name of the receiver. (Range: 1-256 characters; Default: None)

5. Sampling must be disabled by setting the time out to 0 before these fields can be configured.

- ◆ **Receiver IP Address⁵** – IP address of the sFlow Collector.
- ◆ **Receiver Port⁵** – The UDP port on which the sFlow Collector is listening for sFlow streams. (Range: 0-65534; Default: 6343)
- ◆ **Timeout** – The time that the sFlow process will continuously send samples to the Collector before resetting all sFlow port parameters. (Range: 0-10000000 seconds, where 0 indicates no time out)

The sFlow parameters affected by this command include the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.
- ◆ **Max Header Size** – Maximum size of the sFlow datagram header. (Range: 64-256 bytes; Default: 128 bytes)
- ◆ **Max Datagram Size** – Maximum size of the sFlow datagram payload. (Range: 200-1500 bytes; Default: 1400 bytes)
- ◆ **Sample Rate** – The number of packets out of which one sample will be taken. (Range: 256-16777215 packets; Default: Disabled)
- ◆ **Polling Interval** – The interval at which counters are added to the sample datagram. (Range: 1-10,000,000 seconds; Default: Disabled)

WEB INTERFACE

To configure flow sampling:

1. Click Interface, sFlow.
2. Select Configure Interface from the Step list.
3. Set the parameters for flow collector, the reset timeout, the payload, the sampling rate and the polling interval.
4. Click Apply.

Figure 59: Configuring Interface Settings for Traffic Flow Sampling

Interface > sFlow

Step: 2. Configure Interface

Port5

Source Status☒ Enabled

Receiver OwnerLamar

Receiver IP Address192.168.0.9

Receiver Port (0-65534)6343

Timeout (0-10000000)0 sec

Max Header Size (64-256)256 bytes

Max Datagram Size (200-1500)1400 bytes

Sample Rate (256-16777215)☒ Sample one packet randomly from 255 packets

Polling Interval (1-10000000)☒ 10 sec

ApplyRevert

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. Data traffic on downlink ports is only forwarded to, and from, uplink ports.

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.

ENABLING TRAFFIC SEGMENTATION Use the Interface > Traffic Segmentation (Configure Global) page to enable traffic segmentation.

CLI REFERENCES

- ◆ ["Configuring Port-based Traffic Segmentation" on page 1148](#)

PARAMETERS

These parameters are displayed:

- ◆ **Status** – Enables port-based traffic segmentation. (Default: Disabled)
- ◆ **Uplink-to-Uplink Mode** – Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions.

- **Blocking** – Blocks traffic between uplink ports assigned to different sessions.
- **Forwarding** – Forwards traffic between uplink ports assigned to different sessions.

WEB INTERFACE

To enable traffic segmentation:

1. Click Interface, Traffic Segmentation.
2. Select Configure Global from the Step list.
3. Mark the Status check box, and set the required uplink-to-uplink mode.
4. Click Apply.

Figure 60: Enabling Traffic Segmentation



The screenshot shows a web interface titled "Interface > Traffic Segmentation". Below the title is a "Step:" dropdown menu with "1. Configure Global" selected. The main configuration area contains two settings: "Status" with a checkbox labeled "Enabled" (which is unchecked), and "Uplink-to-Uplink Mode" with a dropdown menu set to "Blocking". At the bottom right of the configuration area are two buttons: "Apply" and "Revert".

**CONFIGURING UPLINK
AND DOWNLINK PORTS**

Use the Interface > Traffic Segmentation (Configure Session) page to assign the downlink and uplink ports to use in the segmented group. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

CLI REFERENCES

- ◆ ["Configuring Port-based Traffic Segmentation" on page 1148](#)

COMMAND USAGE

- ◆ When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 11: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured on the Configure Global page (see [page 187](#)).

- ◆ 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.
- ◆ A port cannot be configured in both an uplink and downlink list.
- ◆ A port can only be assigned to one traffic-segmentation session.
- ◆ 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.

PARAMETERS

These parameters are displayed:

- ◆ **Session ID** – Traffic segmentation session. (Range: 1-4)
- ◆ **Direction** – Adds an interface to the segmented group by setting the direction to uplink or downlink. (Default: Uplink)

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-16)

WEB INTERFACE

To configure the members of the traffic segmentation group:

1. Click Interface, Traffic Segmentation.
2. Select Configure Session from the Step list.
3. Select Add from the Action list.
4. Enter the session ID, set the direction to uplink or downlink, and select the interface to add.
5. Click Apply.

Figure 61: Configuring Members for Traffic Segmentation

The screenshot shows the 'Interface > Traffic Segmentation' web interface. At the top, there's a breadcrumb 'Interface > Traffic Segmentation'. Below it, a 'Step:' dropdown is set to '2. Configure Session' and an 'Action:' dropdown is set to 'Add'. The main form has three sections: 'Session ID (1-4)' with a text input containing '1'; 'Direction' with a dropdown menu set to 'Uplink'; and 'Interface' with two radio button options. The 'Port (1-28)' option is selected, with a text input containing '1'. The 'Trunk (1-16)' option is unselected. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the members of the traffic segmentation group:

1. Click Interface, Traffic Segmentation.
2. Select Configure Session from the Step list.
3. Select Show from the Action list.

Figure 62: Showing Traffic Segmentation Members

The screenshot shows the 'Interface > Traffic Segmentation' web interface with the 'Action:' dropdown set to 'Show'. Below the form, there's a 'Session List' section with a 'Total: 2' indicator. It contains a table with 4 columns: a checkbox column, 'Session ID', 'Direction', and 'Interface'. There are two rows of data. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Session ID	Direction	Interface
<input type="checkbox"/>	1	Uplink	Unit 1 / Port 1
<input type="checkbox"/>	1	Downlink	Unit 1 / Port 2

VLAN TRUNKING

Use the Interface > VLAN Trunking page to allow unknown VLAN groups to pass through the specified interface.

CLI REFERENCES

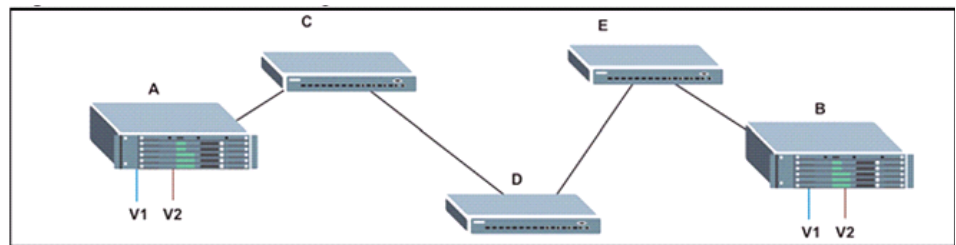
- ◆ ["vlan-trunking" on page 1132](#)

COMMAND USAGE

- ◆ Use this feature to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

Figure 63: Configuring VLAN Trunking



Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- ◆ VLAN trunking is mutually exclusive with the "access" switchport mode (see ["Adding Static Members to VLANs" on page 199](#)). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
- ◆ To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).
- ◆ If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-16)
- ◆ **VLAN Trunking Status** – Enables VLAN trunking on the selected interface.

WEB INTERFACE

To enable VLAN trunking on a port or trunk:

1. Click Interface, VLAN Trunking.
2. Click Port or Trunk to specify the interface type.
3. Enable VLAN trunking on any of the ports or on a trunk.
4. Click Apply.

Figure 64: Configuring VLAN Trunking

The screenshot shows a web interface titled "Interface > VLAN Trunking". Below the title, there are two radio buttons: "Port" (selected) and "Trunk". Below this, it says "Port VLAN Trunking List Total: 28". There are three numbered tabs: 1, 2, and 3. The main table has two columns: "Port" and "VLAN Trunking Status". The table lists ports 1 through 10. Port 1 has a checked checkbox and the text "Enabled". Ports 2 through 10 have unchecked checkboxes and the text "Enabled". At the bottom of the table, there are two buttons: "Apply" and "Revert".

Port	VLAN Trunking Status
1	<input checked="" type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled
6	<input type="checkbox"/> Enabled
7	<input type="checkbox"/> Enabled
8	<input type="checkbox"/> Enabled
9	<input type="checkbox"/> Enabled
10	<input type="checkbox"/> Enabled

This chapter includes the following topics:

- ◆ [IEEE 802.1Q VLANs](#) – Configures static and dynamic VLANs.
- ◆ [IEEE 802.1Q Tunneling](#) – Configures QinQ tunneling to maintain customer-specific VLAN and Layer 2 protocol configurations across a service provider network, even when different customers use the same internal VLAN IDs.
- ◆ [Protocol VLANs](#) – Configures VLAN groups based on specified protocols.
- ◆ [IP Subnet VLANs](#) – Maps untagged ingress frames to a specified VLAN if the source address is found in the IP subnet-to-VLAN mapping table.
- ◆ [MAC-based VLANs](#) – Maps untagged ingress frames to a specified VLAN if the source MAC address is found in the IP MAC address-to-VLAN mapping table.
- ◆ [VLAN Mirroring](#) – Mirrors traffic from one or more source VLANs to a target port.
- ◆ [VLAN Translation](#) – Maps VLAN IDs between the customer and the service provider.

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q 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.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- ◆ Up to 4093 VLANs based on the IEEE 802.1Q standard
- ◆ Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- ◆ Port overlapping, allowing a port to participate in multiple VLANs
- ◆ End stations can belong to multiple VLANs
- ◆ Passing traffic between VLAN-aware and VLAN-unaware devices
- ◆ Priority tagging

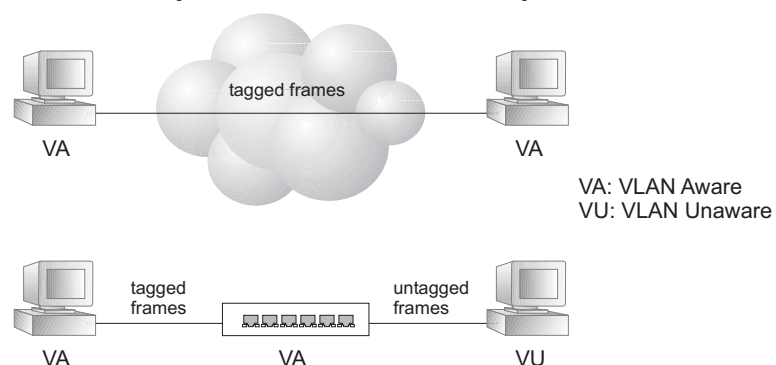
Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.



NOTE: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

Figure 65: VLAN Compliant and VLAN Non-compliant Devices



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (i.e., static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

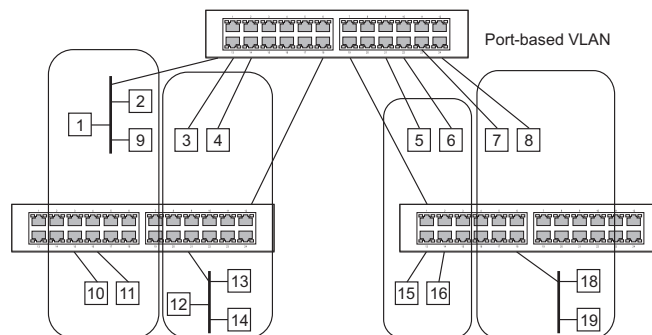
Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on end station requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.



NOTE: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in ["Adding Static Members to VLANs" on page 199](#)). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Figure 66: Using GVRP



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

CONFIGURING VLAN GROUPS

Use the VLAN > Static (Add) page to create or remove VLAN groups, set administrative status, or specify Remote VLAN type (see ["Configuring Remote Port Mirroring" on page 158](#)). To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

CLI REFERENCES

- ◆ ["Editing VLAN Groups" on page 1125](#)

PARAMETERS

These parameters are displayed:

Add

- ◆ **VLAN ID** – ID of VLAN or range of VLANs (1-4093).
VLAN 1 is the default untagged VLAN.
- ◆ **Status** – Enables or disables the specified VLAN.

- ◆ **Remote VLAN** – Reserves this VLAN for RSPAN (see ["Configuring Remote Port Mirroring" on page 158](#)).
- ◆ **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN (see ["Setting the Switch's IP Address \(IP Version 4\)" on page 617](#)).

Modify

- ◆ **VLAN ID** – ID of configured VLAN (1-4093).
- ◆ **VLAN Name** – Name of the VLAN (1 to 32 characters).
- ◆ **Status** – Enables or disables the specified VLAN.
- ◆ **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN.

Show

- ◆ **VLAN ID** – ID of configured VLAN.
- ◆ **VLAN Name** – Name of the VLAN.
- ◆ **Status** – Operational status of configured VLAN.
- ◆ **Remote VLAN** – Shows if RSPAN is enabled on this VLAN (see ["Configuring Remote Port Mirroring" on page 158](#)).
- ◆ **L3 Interface** – Shows if the interface supports Layer 3 configuration.

WEB INTERFACE

To create VLAN groups:

1. Click VLAN, Static.
2. Select Add from the Action list.
3. Enter a VLAN ID or range of IDs.
4. Mark Enabled to configure the VLAN as operational.
5. Specify whether the VLANs are to be used for remote port mirroring.
6. Enable the L3 Interface field to specify that a VLAN will be used as a Layer 3 interface.
7. Click Apply.

Figure 67: Creating Static VLANs

VLAN > Static

Action: Add

VLAN ID (1-4093) 2 -

Status ☒ Enabled

Remote VLAN ☐ Enabled

Apply Revert

To modify the configuration settings for VLAN groups:

1. Click VLAN, Static.
2. Select Modify from the Action list.
3. Select the identifier of a configured VLAN.
4. Modify the VLAN name, operational status, or Layer 3 Interface status as required.
5. Click Apply.

Figure 68: Modifying Settings for Static VLANs

VLAN > Static

Action: Modify

VLAN ID (1-4093) 2

VLAN Name R&D

Status ☒ Enabled

L3 Interface ☒ Enabled

Apply Revert

To show the configuration settings for VLAN groups:

1. Click VLAN, Static.
2. Select Show from the Action list.

Figure 69: Showing Static VLANs

VLAN > Static

Action: Show

Static VLAN List Total: 2

	VLAN ID	VLAN Name	Status	Remote VLAN	L3 Interface
<input type="checkbox"/>	1	DefaultVlan	Enabled	Disabled	Enabled
<input type="checkbox"/>	2	R&D	Enabled	Disabled	Enabled

Delete Revert

**ADDING STATIC
MEMBERS TO VLANs**

Use the VLAN > Static pages to configure port members for the selected VLAN index, interface, or a range of interfaces. Use the menus for editing port members to configure the VLAN behavior for specific interfaces, including the mode of operation (Hybrid or 1Q Trunk), the default VLAN identifier (PVID), accepted frame types, and ingress filtering. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged if they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

CLI REFERENCES

- ◆ ["Configuring VLAN Interfaces" on page 1127](#)
- ◆ ["Displaying VLAN Information" on page 1134](#)

PARAMETERS

These parameters are displayed:

Edit Member by VLAN

- ◆ **VLAN** – ID of configured VLAN (1-4093).
- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-16)
- ◆ **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
 - **Access** - Sets the port to operate as an untagged interface. The port transmits and receives untagged frames on a single VLAN only.
Access mode is mutually exclusive with VLAN trunking (see ["VLAN Trunking" on page 191](#)). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
 - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
 - **1Q 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.
- ◆ **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

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.

- ◆ **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)
- ◆ **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
 - 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 STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- ◆ **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
 - **Tagged:** Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
 - **Untagged:** Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
 - **Forbidden:** Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see “Automatic VLAN Registration” on page 195.
 - **None:** Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.



NOTE: VLAN 1 is the default untagged VLAN containing all ports on the switch, and membership type can only be modified by first assigning a port to another VLAN and then reassigning the default port VLAN ID.

Edit Member by Interface

All parameters are the same as those described under the preceding section for Edit Member by VLAN.

Edit Member by Interface Range

All parameters are the same as those described under the earlier section for Edit Member by VLAN, except for the items shown below.

- ◆ **Port Range** – Displays a list of ports. (Range: 1-28/52)
- ◆ **Trunk Range** – Displays a list of ports. (Range: 1-16)



NOTE: The PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.

WEB INTERFACE

To configure static members by the VLAN index:

1. Click VLAN, Static.
2. Select a VLAN from the scroll-down list.
3. Select Edit Member by VLAN from the Action list.
4. Set the Interface type to display as Port or Trunk.
5. Modify the settings for any interface as required. Remember that Membership Type cannot be changed until an interface has been added to another VLAN and the PVID changed to anything other than 1.
6. Click Apply.

Figure 70: Configuring Static Members by VLAN Index

The screenshot shows the 'VLAN > Static' configuration page. The 'Action' dropdown is set to 'Edit Member by VLAN'. The 'VLAN' dropdown is set to '1'. The 'Interface' radio buttons are set to 'Port'. Below this is the 'Static VLAN Port Member List' table with a total of 28 members. The table has columns for Port, Mode, PVID, Acceptable Frame Type, Ingress Filtering, and Membership Type (Tagged, Untagged, Forbidden, None). The first five rows of the table are visible, showing ports 1 through 5, all in 'Hybrid' mode with PVID '1' and 'All' acceptable frame types. Ingress filtering is disabled for all ports. The 'Tagged' membership type is selected for all ports.

Port	Mode	PVID	Acceptable Frame Type	Ingress Filtering	Membership Type			
					Tagged	Untagged	Forbidden	None
1	Hybrid	1	All	<input type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	Hybrid	1	All	<input type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	Hybrid	1	All	<input type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	Hybrid	1	All	<input type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	Hybrid	1	All	<input type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To configure static members by interface:

1. Click VLAN, Static.
2. Select Edit Member by Interface from the Action list.
3. Select a port or trunk configure.
4. Modify the settings for any interface as required.
5. Click Apply.

Figure 71: Configuring Static VLAN Members by Interface

VLAN > Static

Action: **Edit Member by Interface**

Interface: ☒ Port **1** ☐ Trunk **1**

Mode: **Hybrid**

PVID: **1**

Acceptable Frame Type: **All**

Ingress Filtering: ☐ Enabled

Static VLAN Membership List Total: 4

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Apply Revert

To configure static members by interface range:

1. Click VLAN, Static.
2. Select Edit Member by Interface Range from the Action list.
3. Set the Interface type to display as Port or Trunk.
4. Enter an interface range.
5. Modify the VLAN parameters as required. Remember that the PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.
6. Click Apply.

Figure 72: Configuring Static VLAN Members by Interface Range

VLAN > Static

Action: Edit Member by Interface Range

Interface: ☒ Port ☐ Trunk

Port Range (1-28): -

Mode: Access

VLAN ID (1-4094): -

Membership Type: ☐ Tagged ☒ Untagged ☐ Forbidden ☐ None

Apply Revert

CONFIGURING DYNAMIC VLAN REGISTRATION

Use the VLAN > Dynamic page to enable GVRP globally on the switch, or to enable GVRP and adjust the protocol timers per interface.

CLI REFERENCES

- ◆ ["GVRP and Bridge Extension Commands" on page 1120](#)
- ◆ ["Configuring VLAN Interfaces" on page 1127](#)

PARAMETERS

These parameters are displayed:

Configure General

- ◆ **GVRP Status** – GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Configure Interface

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-16)
- ◆ **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (using the Configure General page). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

GVRP cannot be enabled for ports set to Access mode (see ["Adding Static Members to VLANs" on page 199](#)).

- ◆ **GVRP Timers** – Timer settings must follow this rule:
 $2 \times (\text{join timer}) < \text{leave timer} < \text{leaveAll timer}$
 - **Join** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
 - **Leave** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
 - **LeaveAll** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

Show Dynamic VLAN – Show VLAN

VLAN ID – Identifier of a VLAN this switch has joined through GVRP.

VLAN Name – Name of a VLAN this switch has joined through GVRP.

Status – Indicates if this VLAN is currently operational.
(Display Values: Enabled, Disabled)

Show Dynamic VLAN – Show VLAN Member

- ◆ **VLAN** – Identifier of a VLAN this switch has joined through GVRP.
- ◆ **Interface** – Displays a list of ports or trunks which have joined the selected VLAN through GVRP.

WEB INTERFACE

To configure GVRP on the switch:

1. Click VLAN, Dynamic.
2. Select Configure General from the Step list.
3. Enable or disable GVRP.
4. Click Apply.

Figure 73: Configuring Global Status of GVRP

VLAN > Dynamic

Step: 1. Configure General

GVRP Status ☒ Enabled

Apply Revert

To configure GVRP status and timers on a port or trunk:

1. Click VLAN, Dynamic.
2. Select Configure Interface from the Step list.
3. Set the Interface type to display as Port or Trunk.
4. Modify the GVRP status or timers for any interface.
5. Click Apply.

Figure 74: Configuring GVRP for an Interface

VLAN > Dynamic

Step: 2. Configure Interface

Interface ☒ Port ☐ Trunk

Port List Total: 28

Port	GVRP Status	GARP Timer (centiseconds)		
		Join (20-1000)	Leave (60-3000)	LeaveAll (500-18000)
1	<input type="checkbox"/> Enabled	20	60	1000
2	<input type="checkbox"/> Enabled	20	60	1000
3	<input checked="" type="checkbox"/> Enabled	20	60	1000
4	<input type="checkbox"/> Enabled	20	60	1000
5	<input type="checkbox"/> Enabled	20	60	1000

To show the dynamic VLAN joined by this switch:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN from the Action list.

Figure 75: Showing Dynamic VLANs Registered on the Switch

The screenshot shows the 'VLAN > Dynamic' configuration page. At the top, there is a 'Step' dropdown menu set to '3. Show Dynamic VLAN' and an 'Action' dropdown menu set to 'Show VLAN'. Below this, the text 'Dynamic VLAN List Total: 2' is displayed. A table with three columns: 'VLAN ID', 'VLAN Name', and 'Status' is shown. The table contains two rows: one for VLAN ID 120 and another for VLAN ID 150, both with the status 'Enabled'.

VLAN ID	VLAN Name	Status
120		Enabled
150		Enabled

To show the members of a dynamic VLAN:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN Members from the Action list.

Figure 76: Showing the Members of a Dynamic VLAN

The screenshot shows the 'VLAN > Dynamic' configuration page. At the top, there is a 'Step' dropdown menu set to '3. Show Dynamic VLAN' and an 'Action' dropdown menu set to 'Show VLAN Member'. Below this, there is a 'VLAN' dropdown menu set to '120'. The text 'Dynamic VLAN Member List Total: 10' is displayed. A table with one column: 'Interface' is shown. The table contains five rows: 'Unit 1 / Port 1', 'Unit 1 / Port 4', 'Unit 1 / Port 10', 'Unit 1 / Port 16', and 'Unit 1 / Port 19'.

Interface
Unit 1 / Port 1
Unit 1 / Port 4
Unit 1 / Port 10
Unit 1 / Port 16
Unit 1 / Port 19

IEEE 802.1Q TUNNELING

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

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

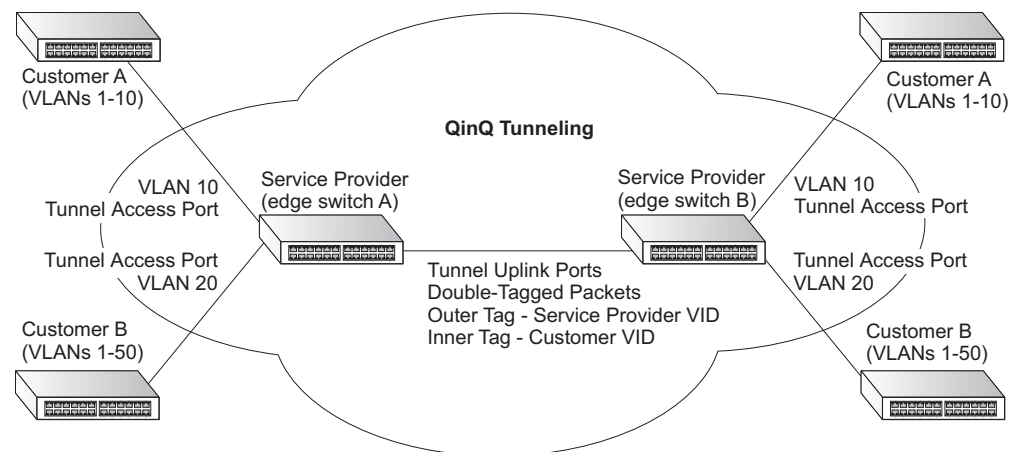
provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

Figure 77: QinQ Operational Concept



Layer 2 Flow for Packets Coming into a Tunnel Access Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. An SPVLAN tag is added to all outbound packets on the SPVLAN interface, no matter how many tags they already have. The switch constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag), unless otherwise defined as described under ["Creating CVLAN to SPVLAN Mapping Entries" on page 211](#). The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.
2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.
3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).
4. The switch sends the packet to the proper egress port.
5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into a Tunnel Uplink Port

An uplink port receives one of the following packets:

- ◆ Untagged
- ◆ One tag (CVLAN or SPVLAN)
- ◆ Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.

3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.
5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The switch sends the packet to the proper egress port.
8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

- ◆ The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes non-customer packets to be forwarded to the SPVLAN.
- ◆ Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.
- ◆ The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.
- ◆ There are some inherent incompatibilities between Layer 2 and Layer 3 switching:
 - Tunnel ports do not support IP Access Control Lists.
 - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
 - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Enable Tunnel Status, and set the Tag Protocol Identifier (TPID) value of the tunnel access port (in the Ethernet Type field). This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. (See ["Enabling QinQ Tunneling on the Switch" on page 210](#).)
2. Create a Service Provider VLAN, also referred to as an SPVLAN (see ["Configuring VLAN Groups" on page 196](#)).
3. Configure the QinQ tunnel access port to Access mode (see ["Adding an Interface to a QinQ Tunnel" on page 213](#)).
4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see ["Adding Static Members to VLANs" on page 199](#)).
5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see ["Adding Static Members to VLANs" on page 199](#)).
6. Configure the QinQ tunnel uplink port to Uplink mode (see ["Adding an Interface to a QinQ Tunnel" on page 213](#)).
7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see ["Adding Static Members to VLANs" on page 199](#)).

ENABLING QINQ TUNNELING ON THE SWITCH

Use the VLAN > Tunnel (Configure Global) page to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

CLI REFERENCES

- ◆ ["Configuring IEEE 802.1Q Tunneling" on page 1135](#)

PARAMETERS

These parameters are displayed:

- ◆ **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)
- ◆ **Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)

Use this field to set a custom 802.1Q ethertype value for the 802.1Q Tunnel TPID. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the 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 (see ["Adding an Interface to a QinQ Tunnel" on page 213](#)). If the port is in normal mode, the TPID is always 8100. If the port is in Access mode, received packets are processed as untagged packets.

WEB INTERFACE

To enable QinQ Tunneling on the switch:

1. Click VLAN, Tunnel.
2. Select Configure Global from the Step list.
3. Enable Tunnel Status, and specify the TPID if a client attached to a tunnel port is using a non-standard ethertype to identify 802.1Q tagged frames.
4. Click Apply.

Figure 78: Enabling QinQ Tunneling

The screenshot shows a web interface for configuring VLAN tunneling. The breadcrumb is 'VLAN > Tunnel'. Below it, a 'Step:' dropdown menu is set to '1. Configure Global'. The main configuration area has two fields: 'Tunnel Status' with a checked checkbox labeled 'Enabled', and 'Ethernet Type' with a text input field containing '8100'. Below the 'Ethernet Type' field is a note: '(800-FFFF, hexadecimal value)'. At the bottom right of the form are two buttons: 'Apply' and 'Revert'.

CREATING CVLAN TO SPVLAN MAPPING ENTRIES

Use the VLAN > Tunnel (Configure Service) page to create a CVLAN to SPVLAN mapping entry.

CLI REFERENCES

- ◆ ["switchport dot1q-tunnel service match cvid" on page 1138](#)

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. By default, the outer tag is based on the default VID of the edge router's ingress port. This process is performed in a transparent manner as described under ["IEEE 802.1Q Tunneling" on page 206](#).
- ◆ 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 Configure Interface page described in the next section to set an interface to access or uplink mode.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Customer VLAN ID** – VLAN ID for the inner VLAN tag. (Range: 1-4094)
- ◆ **Service VLAN ID** – VLAN ID for the outer VLAN tag. (Range: 1-4093)

WEB INTERFACE

To configure a mapping entry:

1. Click VLAN, Tunnel.
2. Select Configure Service from the Step list.
3. Select Add from the Action list.
4. Select an interface from the Port list.
5. Specify the CVID to SVID mapping for packets exiting the specified port.
6. Click Apply.

Figure 79: Configuring CVLAN to SPVLAN Mapping Entries

The screenshot shows a web interface for configuring VLAN tunnels. The breadcrumb is 'VLAN > Tunnel'. The 'Step' dropdown is set to '2. Configure Service' and the 'Action' dropdown is set to 'Add'. There are three input fields: 'Port' with a dropdown menu showing '1', 'Customer VLAN ID (1-4094)' with a text box containing '2', and 'Service VLAN ID (1-4093)' with a text box containing '99'. At the bottom right are 'Apply' and 'Revert' buttons.

To show the mapping table:

1. Click VLAN, Tunnel.
2. Select Configure Service from the Step list.
3. Select Show from the Action list.
4. Select an interface from the Port list.

Figure 80: Showing CVLAN to SPVLAN Mapping Entries

The screenshot shows the 'VLAN > Tunnel' configuration page. At the top, there's a breadcrumb 'VLAN > Tunnel' and a help icon. Below that, a 'Step:' dropdown is set to '2. Configure Service' and an 'Action:' dropdown is set to 'Show'. A 'Port' dropdown is set to '1'. Below this is a section titled 'Tunnel Service Subscriptions List' with a 'Total: 2' indicator. It contains a table with two columns: 'Customer VLAN ID' and 'Service VLAN ID'. The table has two rows: the first row shows '1' for both, and the second row shows '2' for Customer and '200' for Service. At the bottom of the table are 'Delete' and 'Revert' buttons.

Customer VLAN ID	Service VLAN ID
1	1
2	200

The preceding example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2. For a more detailed example, see the [switchport dot1q-tunnel service match cvid](#) command on [page 1138](#).

ADDING AN INTERFACE TO A QINQ TUNNEL

Follow the guidelines under ["Enabling QinQ Tunneling on the Switch"](#) to set up a QinQ tunnel on the switch. Then use the VLAN > Tunnel (Configure Interface) page to set the tunnel mode for any participating interface.

CLI REFERENCES

- ◆ ["Configuring IEEE 802.1Q Tunneling" on page 1135](#)

COMMAND USAGE

- ◆ Use the Configure Global page to set the switch to QinQ mode before configuring a tunnel access port or tunnel uplink port (see ["Enabling QinQ Tunneling on the Switch" on page 210](#)). Also set the Tag Protocol Identifier (TPID) value of the tunnel access port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.
- ◆ Then use the Configure Interface page to set the access interface on the edge switch to Access mode, and set the uplink interface on the switch attached to the service provider network to Uplink mode.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-16)
- ◆ **Mode** – Sets the VLAN membership mode of the port.
 - **None** – The port operates in its normal VLAN mode. (This is the default.)
 - **Access** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
 - **Uplink** – Configures QinQ tunneling for an uplink port to another device within the service provider network.

WEB INTERFACE

To add an interface to a QinQ tunnel:

1. Click VLAN, Tunnel.
2. Select Configure Interface from the Step list.
3. Set the mode for any tunnel access port to Access and the tunnel uplink port to Uplink.
4. Click Apply.

Figure 81: Adding an Interface to a QinQ Tunnel

VLAN > Tunnel

Step: 3. Configure Interface

Interface ☒ Port ☐ Trunk

802.1Q Tunnel Port List Total: 28

Port	Mode
1	Uplink
2	Access
3	None
4	None
5	None

PROTOCOL 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 being used by the inbound packets.

COMMAND USAGE

- ◆ To configure protocol-based VLANs, follow these steps:
 1. First configure VLAN groups for the protocols you want to use ([page 1125](#)). 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 Configure Protocol (Add) page.
 3. Then map the protocol for each interface to the appropriate VLAN using the Configure Interface (Add) page.
- ◆ 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.

CONFIGURING PROTOCOL VLAN GROUPS

Use the VLAN > Protocol (Configure Protocol - Add) page to create protocol groups.

CLI REFERENCES

- ◆ "[protocol-vlan protocol-group \(Configuring Groups\)](#)" on [page 1153](#)

PARAMETERS

These parameters are displayed:

- ◆ **Frame Type** – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.
- ◆ **Protocol Type** – Specifies the protocol type to match. The available options are IP, ARP, RARP and IPv6. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX Raw.
- ◆ **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)



NOTE: Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN (VLAN 1) that has been configured with the switch's administrative IP. IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, network access can be regained by removing the offending Protocol VLAN rule via the console. Alternately, the switch can be power-cycled, however all unsaved configuration changes will be lost.

WEB INTERFACE

To configure a protocol group:

1. Click VLAN, Protocol.
2. Select Configure Protocol from the Step list.
3. Select Add from the Action list.
4. Select an entry from the Frame Type list.
5. Select an entry from the Protocol Type list.
6. Enter an identifier for the protocol group.
7. Click Apply.

Figure 82: Configuring Protocol VLANs

VLAN > Protocol

Step: 1. Configure Protocol Action: Add

Frame Type Ethernet

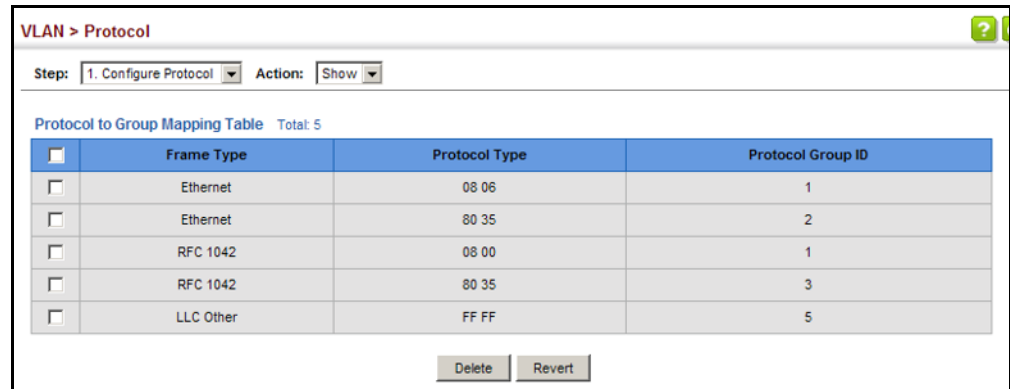
Protocol Type 08 06 (ARP)

Protocol Group ID (1-2147483647) 1

Apply Revert

To configure a protocol group:

1. Click VLAN, Protocol.
2. Select Configure Protocol from the Step list.
3. Select Show from the Action list.

Figure 83: Displaying Protocol VLANs


The screenshot shows the 'VLAN > Protocol' configuration page. At the top, there's a header 'VLAN > Protocol' with a help icon. Below it, a 'Step:' dropdown is set to '1. Configure Protocol' and an 'Action:' dropdown is set to 'Show'. The main section is titled 'Protocol to Group Mapping Table' with a 'Total: 5' indicator. It contains a table with 4 columns: a checkbox, 'Frame Type', 'Protocol Type', and 'Protocol Group ID'. The table lists 5 entries: Ethernet (08 06) to group 1, Ethernet (80 35) to group 2, RFC 1042 (08 00) to group 1, RFC 1042 (80 35) to group 3, and LLC Other (FF FF) to group 5. At the bottom right are 'Delete' and 'Revert' buttons.

<input type="checkbox"/>	Frame Type	Protocol Type	Protocol Group ID
<input type="checkbox"/>	Ethernet	08 06	1
<input type="checkbox"/>	Ethernet	80 35	2
<input type="checkbox"/>	RFC 1042	08 00	1
<input type="checkbox"/>	RFC 1042	80 35	3
<input type="checkbox"/>	LLC Other	FF FF	5

MAPPING PROTOCOL GROUPS TO INTERFACES

Use the VLAN > Protocol (Configure Interface - Add) page to map a protocol group to a VLAN for each interface that will participate in the group.

CLI REFERENCES

- ◆ ["protocol-vlan protocol-group \(Configuring Interfaces\)" on page 1154](#)

COMMAND USAGE

- ◆ When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN menus such as the VLAN Static table ([page 199](#)), these interfaces will admit traffic of any protocol type into the associated VLAN.
- ◆ 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.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-16)
- ◆ **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)

- ◆ **VLAN ID** – VLAN to which matching protocol traffic is forwarded.
(Range: 1-4093)
- ◆ **Priority** – The priority assigned to untagged ingress traffic.
(Range: 0-7, where 7 is the highest priority)

WEB INTERFACE

To map a protocol group to a VLAN for a port or trunk:

1. Click VLAN, Protocol.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Select a port or trunk.
5. Enter the identifier for a protocol group.
6. Enter the corresponding VLAN to which the protocol traffic will be forwarded.
7. Set the priority to assign to untagged ingress frames.
8. Click Apply.

Figure 84: Assigning Interfaces to Protocol VLANs

The screenshot shows a web interface for configuring protocol VLANs. The breadcrumb is 'VLAN > Protocol'. The 'Step' dropdown is set to '2. Configure Interface' and the 'Action' dropdown is set to 'Add'. The 'Interface' section has radio buttons for 'Port' (selected) and 'Trunk'. The 'Port' dropdown is set to '1'. Below this are three input fields: 'Protocol Group ID' with a dropdown set to '1', 'VLAN ID (1-4093)' which is empty, and 'Priority (0-7)' which is empty. At the bottom right are 'Apply' and 'Revert' buttons.

To show the protocol groups mapped to a port or trunk:

1. Click VLAN, Protocol.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port or trunk.

Figure 85: Showing the Interface to Protocol Group Mapping

The screenshot shows the 'VLAN > Protocol' configuration page. At the top, there's a breadcrumb 'VLAN > Protocol' and a help icon. Below that, a 'Step:' dropdown is set to '2. Configure Interface' and an 'Action:' dropdown is set to 'Show'. Under the 'Interface' section, 'Port 1' is selected with a radio button, and 'Trunk' is selected with a dropdown arrow. Below this is the 'Port To Protocol Group Mapping Table' with a 'Total: 1' count. The table has three columns: 'Protocol Group ID', 'VLAN ID', and 'Priority'. It contains one entry with Protocol Group ID '1', VLAN ID '2', and Priority '0'. At the bottom of the table are 'Delete' and 'Revert' buttons.

Protocol Group ID	VLAN ID	Priority
1	2	0

CONFIGURING IP SUBNET VLANs

Use the VLAN > IP Subnet page to configure IP subnet-based VLANs.

When using port-based 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).

CLI REFERENCES

- ◆ ["Configuring IP Subnet VLANs" on page 1156](#)

COMMAND USAGE

- ◆ Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a 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, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

PARAMETERS

These parameters are displayed:

- ◆ **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- ◆ **Subnet Mask** – This mask identifies the host address bits of the IP subnet.
- ◆ **VLAN** – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4093)
- ◆ **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

WEB INTERFACE

To map an IP subnet to a VLAN:

1. Click VLAN, IP Subnet.
2. Select Add from the Action list.
3. Enter an address in the IP Address field.
4. Enter a mask in the Subnet Mask field.
5. Enter the identifier in the VLAN field. Note that the specified VLAN need not already be configured.
6. Enter a value to assign to untagged frames in the Priority field.
7. Click Apply.

Figure 86: Configuring IP Subnet VLANs

The screenshot shows a web interface for configuring IP Subnet VLANs. The title bar reads "VLAN > IP Subnet". Below the title bar, there is an "Action:" label followed by a dropdown menu set to "Add". The main configuration area contains four rows of input fields: "IP Address" with the value "192.168.1.0", "Subnet Mask" with the value "255.255.255.0", "VLAN (1-4093)" with the value "10", and "Priority (0-7)" which is empty. At the bottom right of the form are two buttons: "Apply" and "Revert".

To show the configured IP subnet VLANs:

1. Click VLAN, IP Subnet.
2. Select Show from the Action list.

Figure 87: Showing IP Subnet VLANs

The screenshot shows a web interface for configuring VLANs. At the top, it says 'VLAN > IP Subnet'. Below this is an 'Action:' dropdown menu set to 'Show'. The main section is titled 'IP Subnet to VLAN Mapping Table' with a 'Total: 1' indicator. It contains a table with the following data:

	IP Address	Subnet Mask	VLAN	Priority
<input type="checkbox"/>	192.168.1.0	255.255.255.0	10	0

Below the table are 'Delete' and 'Revert' buttons.

CONFIGURING MAC-BASED VLANs

Use the VLAN > MAC-Based page to configure VLAN based on MAC addresses. The MAC-based VLAN feature assigns VLAN IDs to ingress untagged frames according to source MAC addresses.

When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN which is mapped to the frame's source MAC address. When no MAC address is matched, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

CLI REFERENCES

- ◆ ["Configuring MAC Based VLANs" on page 1158](#)

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.

PARAMETERS

These parameters are displayed:

- ◆ **MAC Address** – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx.
- ◆ **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4093)
- ◆ **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

WEB INTERFACE

To map a MAC address to a VLAN:

1. Click VLAN, MAC-Based.
2. Select Add from the Action list.
3. Enter an address in the MAC Address field.
4. Enter an identifier in the VLAN field. Note that the specified VLAN need not already be configured.
5. Enter a value to assign to untagged frames in the Priority field.
6. Click Apply.

Figure 88: Configuring MAC-Based VLANs

VLAN > MAC-Based

Action: Add

MAC Address: 00-ab-cd-11-22-33

VLAN (1-4093): 10

Priority (0-7):

Apply Revert

To show the MAC addresses mapped to a VLAN:

1. Click VLAN, MAC-Based.
2. Select Show from the Action list.

Figure 89: Showing MAC-Based VLANs

VLAN > MAC-Based

Action: Show

MAC-Based VLAN List Total: 1

	MAC Address	VLAN	Priority
<input type="checkbox"/>	00-AB-CD-11-22-33	10	0

Delete Revert

CONFIGURING VLAN MIRRORING

Use the VLAN > Mirror (Add) page to mirror traffic from one or more source VLANs to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source VLAN(s) in a completely unobtrusive manner.

CLI REFERENCES

- ◆ ["Port Mirroring Commands" on page 1013](#)

COMMAND USAGE

- ◆ All active ports in a source VLAN are monitored for ingress traffic only.
- ◆ All VLAN mirror sessions must share the same target port, preferably one that is not a member of the source VLAN.
- ◆ When VLAN mirroring and port mirroring are both enabled, they must use the same target port.
- ◆ 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 mirrored VLAN.
- ◆ The target port receives traffic from all monitored source VLANs and can become congested. Some mirror traffic may therefore be dropped from the target port.
- ◆ When mirroring VLAN traffic or packets based on a source MAC address (see ["Configuring MAC Address Mirroring" on page 232](#)), the target port cannot be set to the same target ports as that used for port mirroring (see ["Configuring Local Port Mirroring" on page 156](#)).
- ◆ When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed:

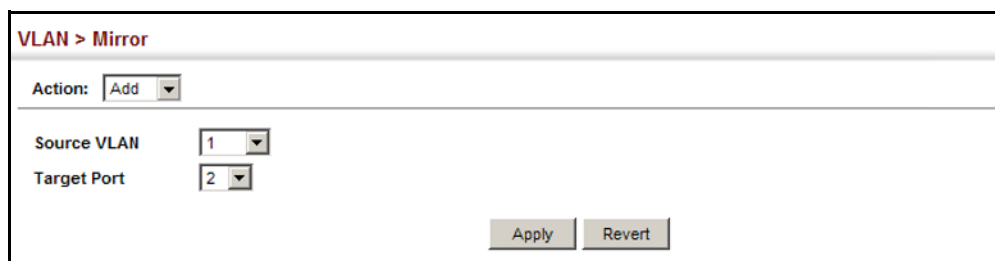
- ◆ **Source VLAN** – A VLAN whose traffic will be monitored.
(Range: 1-4093)
- ◆ **Target Port** – The destination port that receives the mirrored traffic from the source VLAN. (Range: 1-28/52)

WEB INTERFACE

To configure VLAN mirroring:

1. Click VLAN, Mirror.
2. Select Add from the Action list.
3. Select the source VLAN, and select a target port.
4. Click Apply.

Figure 90: Configuring VLAN Mirroring

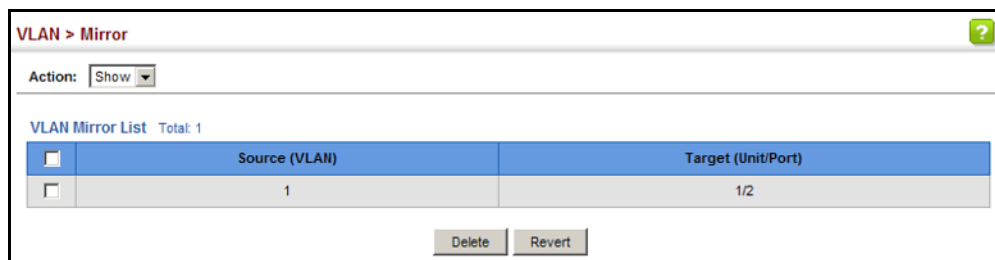


The screenshot shows the 'VLAN > Mirror' configuration page. At the top, the title is 'VLAN > Mirror'. Below the title, there is an 'Action:' dropdown menu with 'Add' selected. Underneath, there are two dropdown menus: 'Source VLAN' with '1' selected and 'Target Port' with '2' selected. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

To show the VLANs to be mirrored:

1. Click VLAN, Mirror.
2. Select Show from the Action list.

Figure 91: Showing the VLANs to Mirror



The screenshot shows the 'VLAN > Mirror' configuration page with the 'Action:' dropdown set to 'Show'. Below the dropdown, there is a table titled 'VLAN Mirror List' with a 'Total: 1' indicator. The table has two columns: 'Source (VLAN)' and 'Target (Unit/Port)'. There is one row in the table with '1' in the 'Source (VLAN)' column and '1/2' in the 'Target (Unit/Port)' column. At the bottom right, there are two buttons: 'Delete' and 'Revert'.

Source (VLAN)	Target (Unit/Port)
1	1/2

CONFIGURING VLAN TRANSLATION

Use the VLAN > Translation (Add) page to map VLAN IDs between the customer and service provider for networks that do not support IEEE 802.1Q tunneling.

CLI REFERENCES

- ◆ ["Configuring VLAN Translation" on page 1146](#)

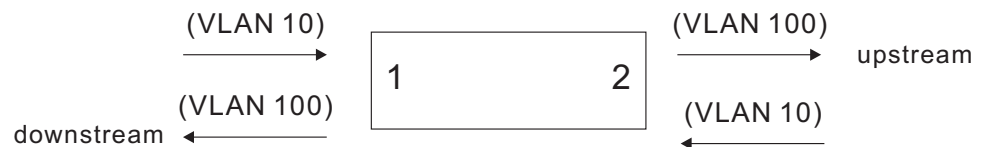
COMMAND USAGE

- ◆ 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.

For example, assume that the upstream switch does not support QinQ tunneling. Select Port 1, and set the Old VLAN to 10 and the New VLAN to 100 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 as shown below.

Figure 92: 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, and the same interface is also configured as a QinQ access port on the VLAN > Tunnel (Configure Interface) page, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port identifier.
- ◆ **Old VLAN** – The original VLAN ID. (Range: 1-4093)
- ◆ **New VLAN** – The new VLAN ID. (Range: 1-4093)

WEB INTERFACE

To configure VLAN translation:

1. Click VLAN, Translation.
2. Select Add from the Action list.
3. Select a port, and enter the original and new VLAN IDs.
4. Click Apply.

Figure 93: Configuring VLAN Translation

VLAN > Translation

Action: Add

Port: 1

Old VLAN (1-4093): 10

New VLAN (1-4093): 100

Apply Revert

To show the mapping entries for VLANs translation:

1. Click VLAN, Translation.
2. Select Show from the Action list.
3. Select a port, and enter the original and new VLAN IDs.

Figure 94: Showing the Entries for VLAN Translation

VLAN > Translation

Action: Show

Port: 1

VLAN Translation Table Total: 1

	Old VLAN	New VLAN
<input type="checkbox"/>	10	100

Delete Revert

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

This chapter describes the following topics:

- ◆ [Static MAC Addresses](#) – Configures static entries in the address table.
- ◆ [Address Aging Time](#) – Sets timeout for dynamically learned entries.
- ◆ [Dynamic Address Cache](#) – Shows dynamic entries in the address table.
- ◆ [MAC Address Mirroring](#) – Mirrors traffic matching a specified source address to a target port.

SETTING STATIC ADDRESSES

Use the MAC Address > Static page to configure static MAC addresses. A static address can be assigned to a specific interface on this switch. 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.

CLI REFERENCES

- ◆ ["mac-address-table static" on page 1054](#)

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 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.
- ◆ Static addresses will not be removed from the address table when a given interface link is down.
- ◆ A static address cannot be learned on another port until the address is removed from the table.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of configured VLAN. (Range: 1-4093)
- ◆ **Interface** – Port or trunk associated with the device assigned a static address.
- ◆ **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- ◆ **Static Status** – Sets the time to retain the specified address.
 - Delete-on-reset - Assignment lasts until the switch is reset.
 - Permanent - Assignment is permanent. (This is the default.)

WEB INTERFACE

To configure a static MAC address:

1. Click MAC Address, Static.
2. Select Add from the Action list.
3. Specify the VLAN, the port or trunk to which the address will be assigned, the MAC address, and the time to retain this entry.
4. Click Apply.

Figure 95: Configuring Static MAC Addresses

The screenshot shows a web interface for configuring static MAC addresses. The title bar reads "MAC Address > Static". Below the title bar, there is a form with the following fields and values:

- Action:** A dropdown menu with "Add" selected.
- VLAN:** A dropdown menu with "1" selected.
- Interface:** Two radio buttons, "Port" and "Trunk". The "Port" radio button is selected, and a dropdown menu next to it shows "1".
- MAC Address:** A text input field containing "00-12-cf-94-34-da".
- Static Status:** A dropdown menu with "Permanent" selected.

At the bottom right of the form, there are two buttons: "Apply" and "Revert".

To show the static addresses in MAC address table:

1. Click MAC Address, Static.
2. Select Show from the Action list.

Figure 96: Displaying Static MAC Addresses

MAC Address > Static

Action: Show

Static MAC Address to Interface Mapping Table Total: 2

<input type="checkbox"/>	MAC Address	VLAN	Interface	Type	Life Time
<input type="checkbox"/>	00-00-0C-00-00-FD	1	CPU	CPU	Delete on Reset
<input type="checkbox"/>	00-12-CF-94-34-DA	1	Unit 1 / Port 1	Config	Permanent

Delete Revert

CHANGING THE AGING TIME

Use the MAC Address > Dynamic (Configure Aging) page to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

CLI REFERENCES

- ◆ ["mac-address-table aging-time" on page 1053](#)

PARAMETERS

These parameters are displayed:

- ◆ **Aging Status** – Enables/disables the function.
- ◆ **Aging Time** – The time after which a learned entry is discarded. (Range: 6-672 seconds; Default: 300 seconds)

WEB INTERFACE

To set the aging time for entries in the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Configure Aging from the Action list.
3. Modify the aging status if required.
4. Specify a new aging time.
5. Click Apply.

Figure 97: Setting the Address Aging Time

MAC Address > Dynamic

Action: Configure Aging

Aging Status ☒ Enabled

Aging Time (6-672) sec

Apply Revert

DISPLAYING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Show Dynamic MAC) page to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

CLI REFERENCES

- ◆ ["show mac-address-table" on page 1055](#)

PARAMETERS

These parameters are displayed:

- ◆ **Sort Key** - You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- ◆ **MAC Address** - Physical address associated with this interface.
- ◆ **VLAN** - ID of configured VLAN (1-4093).
- ◆ **Interface** - Indicates a port or trunk.
- ◆ **Type** - Shows that the entries in this table are learned.
- ◆ **Life Time** - Shows the time to retain the specified address.

WEB INTERFACE

To show the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Show Dynamic MAC from the Action list.
3. Select the Sort Key (MAC Address, VLAN, or Interface).
4. Enter the search parameters (MAC Address, VLAN, or Interface).
5. Click Query.

Figure 98: Displaying the Dynamic MAC Address Table

The screenshot shows the 'MAC Address > Dynamic' configuration page. At the top, there is a breadcrumb 'MAC Address > Dynamic' and a help icon. Below this is an 'Action:' dropdown menu set to 'Show Dynamic MAC'. Under 'Query by:', there is a 'Sort Key' dropdown set to 'MAC Address'. Below that are three checkboxes: 'MAC Address', 'VLAN', and 'Interface'. The 'MAC Address' checkbox is selected. To the right of these checkboxes are input fields: a text box for MAC Address, a dropdown for VLAN (set to '1'), and radio buttons for 'Port' (selected) and 'Trunk' (set to '1'). A 'Query' button is located to the right of these fields. Below the query fields is a section titled 'Dynamic MAC Address List' with a 'Total: 2' indicator. This section contains a table with the following data:

MAC Address	VLAN	Interface	Type	Life Time
00-E0-29-94-34-64	1	Unit 1 / Port 1	Learn	Delete on Timeout
70-72-CF-32-DD-FF	1	Unit 1 / Port 1	Learn	Delete on Timeout

CLEARING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Clear Dynamic MAC) page to remove any learned entries from the forwarding database.

CLI REFERENCES

- ◆ ["clear mac-address-table dynamic" on page 1055](#)

PARAMETERS

These parameters are displayed:

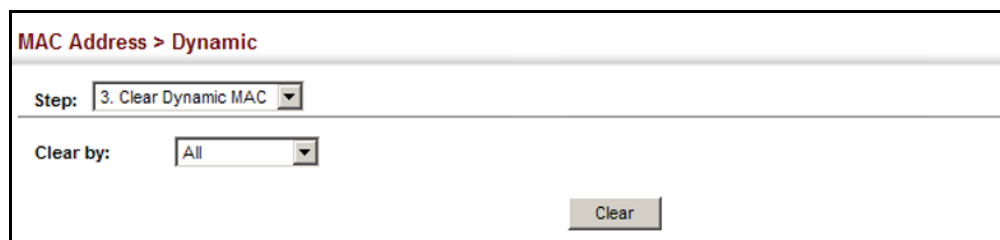
- ◆ **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or trunk.

WEB INTERFACE

To clear the entries in the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Clear Dynamic MAC from the Action list.
3. Select the method by which to clear the entries (i.e., All, MAC Address, VLAN, or Interface).
4. Enter information in the additional fields required for clearing entries by MAC Address, VLAN, or Interface.
5. Click Clear.

Figure 99: Clearing Entries in the Dynamic MAC Address Table



The screenshot shows a web interface for configuring MAC addresses. The breadcrumb trail is "MAC Address > Dynamic". Below this, there is a "Step:" label followed by a dropdown menu currently showing "3. Clear Dynamic MAC". Underneath, there is a "Clear by:" label followed by a dropdown menu currently showing "All". At the bottom right of the form area is a "Clear" button.

CONFIGURING MAC ADDRESS MIRRORING

Use the MAC Address > Mirror (Add) page to mirror traffic matching a specified source address from any port on the switch to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

CLI REFERENCES

- ◆ ["Local Port Mirroring Commands" on page 1013](#)

COMMAND USAGE

- ◆ 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.
- ◆ All mirror sessions must share the same destination port.
- ◆ Spanning Tree BPDU packets are not mirrored to the target port.
- ◆ When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see ["Spanning Tree Algorithm" on page 235](#)).
- ◆ When mirroring VLAN traffic (see ["Configuring VLAN Mirroring" on page 223](#)) or packets based on a source MAC address, the target port cannot be set to the same target ports as that used for port mirroring (see ["Configuring Local Port Mirroring" on page 156](#)).
- ◆ When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed:

- ◆ **Source MAC** – MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

- ◆ **Target Port** – The port that will mirror the traffic from the source port.
(Range: 1-28/52)

WEB INTERFACE

To mirror packets based on a MAC address:

1. Click MAC Address, Mirror.
2. Select Add from the Action list.
3. Specify the source MAC address and destination port.
4. Click Apply.

Figure 100: Mirroring Packets Based on the Source MAC Address

The screenshot shows the 'MAC Address > Mirror' configuration page. The 'Action' dropdown is set to 'Add'. The 'Source MAC' field contains the value '11-22-33-44-55-66'. The 'Target Port' dropdown is set to '2'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the MAC addresses to be mirrored:

1. Click MAC Address, Mirror.
2. Select Show from the Action list.

Figure 101: Showing the Source MAC Addresses to Mirror

The screenshot shows the 'MAC Address > Mirror' configuration page with the 'Action' dropdown set to 'Show'. Below the form fields, there is a table titled 'MAC Mirror List' with a 'Total: 1' indicator. The table has two columns: 'Source (MAC)' and 'Target (Unit/Port)'. The first row shows the source MAC '11-22-33-44-55-66' and target '1/2'. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Source (MAC)	Target (Unit/Port)
<input type="checkbox"/>	11-22-33-44-55-66	1/2

This chapter describes the following basic topics:

- ◆ [Loopback Detection](#) – Configures detection and response to loopback BPDUs.
- ◆ [Global Settings for STA](#) – Configures global bridge settings for STP, RSTP and MSTP.
- ◆ [Interface Settings for STA](#) – Configures interface settings for STA, including priority, path cost, link type, and designation as an edge port.
- ◆ [Global Settings for MSTP](#) – Sets the VLANs and associated priority assigned to an MST instance
- ◆ [Interface Settings for MSTP](#) – Configures interface settings for MSTP, including priority and path cost.

OVERVIEW

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.

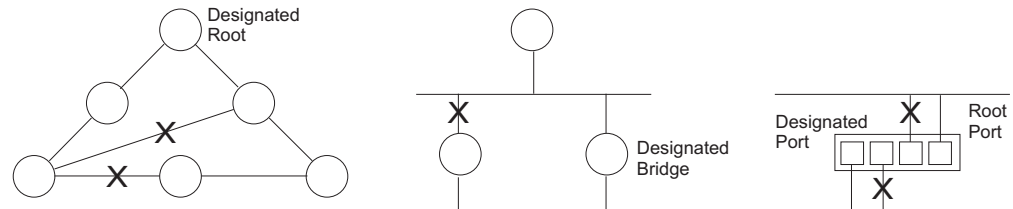
The spanning tree algorithms supported by this switch include these versions:

- ◆ STP – Spanning Tree Protocol (IEEE 802.1D)
- ◆ RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- ◆ MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the

lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Figure 102: STP Root Ports and Designated Ports

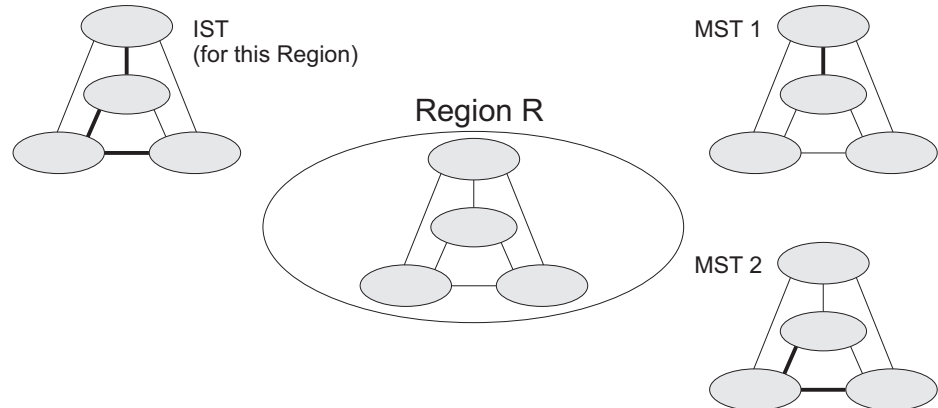


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

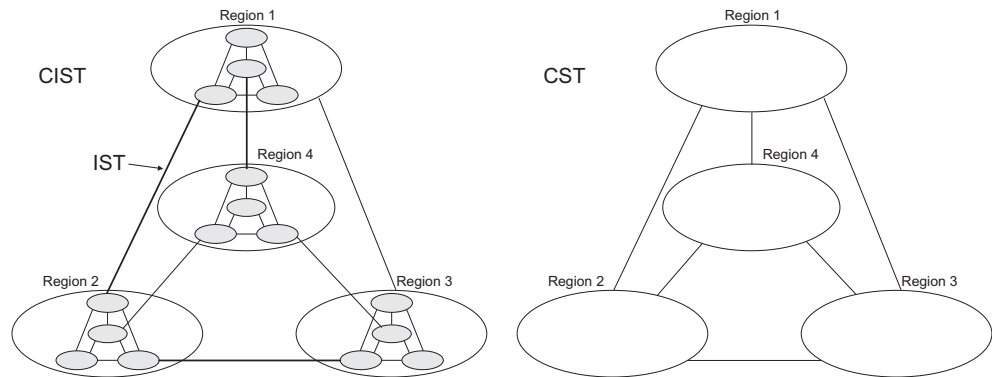
MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.

Figure 103: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree



An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including the Region Name, Revision Level and Configuration Digest – see ["Configuring Multiple Spanning Trees" on page 253](#)). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

Figure 104: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree



MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

CONFIGURING LOOPBACK DETECTION

Use the Spanning Tree > Loopback Detection page to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives its own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface 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 interface receives any other BPDU except for its own, or;
- ◆ The interfaces's link status changes to link down and then link up again, or;
- ◆ The interface ceases to receive its own BPDUs in a forward delay interval.



NOTE: If loopback detection is not enabled and an interface receives its own BPDU, then the interface will drop the loopback BPDU according to IEEE Standard 802.1w-2001 9.3.4 (Note 1).

NOTE: Loopback detection will not be active if Spanning Tree is disabled on the switch.

NOTE: When configured for manual release mode, then a link down/up event will not release the port from the discarding state.

CLI REFERENCES

- ◆ ["Spanning Tree Commands" on page 1059](#)

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Status** – Enables loopback detection on this interface. (Default: Enabled)
- ◆ **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- ◆ **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- ◆ **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- ◆ **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)

- ◆ **Shutdown Interval** – The duration to shut down the interface.
(Range: 60-86400 seconds; Default: 60 seconds)

If an interface is shut down due to a detected loopback, and the release mode is set to "Auto," the selected interface will be automatically enabled when the shutdown interval has expired.

If an interface is shut down due to a detected loopback, and the release mode is set to "Manual," the interface can be re-enabled using the Release button.

WEB INTERFACE

To configure loopback detection:

1. Click Spanning Tree, Loopback Detection.
2. Click Port or Trunk to display the required interface type.
3. Modify the required loopback detection attributes.
4. Click Apply

Figure 105: Configuring Port Loopback Detection

Spanning Tree > Loopback Detection

Interface ☒ Port ☐ Trunk

Loopback Detection Port List Total: 28

Port	Status	Trap	Release Mode	Release	Action	Shutdown Interval (60-86400 sec)
1	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Block	
2	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Block	
3	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Block	
4	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Block	
5	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Manual	Release	Shutdown	60

CONFIGURING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Configure) page to configure global settings for the spanning tree that apply to the entire switch.

CLI REFERENCES

- ◆ ["Spanning Tree Commands" on page 1059](#)

COMMAND USAGE

- ◆ Spanning Tree Protocol⁶

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 Protocol⁶

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 (i.e., STP 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

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.

- 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.

6. STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

- 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.

PARAMETERS

These parameters are displayed:

Basic Configuration of Global Settings

- ◆ **Spanning Tree Status** – Enables/disables STA on this switch.
(Default: Enabled)
- ◆ **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
 - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
 - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
 - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- ◆ **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority 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. (Note that lower numeric values indicate higher priority.)
 - Default: 32768
 - Range: 0-61440, in steps of 4096
 - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
- ◆ **BPDU Flooding** – 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.
 - To VLAN: Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID). This is the default.
 - To All: Floods BPDUs to all other ports on the switch.

The setting has no effect if BPDU flooding is disabled on a port (see ["Configuring Interface Settings for STA"](#)).

Advanced Configuration Settings

The following attributes are based on RSTP, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP, and also apply to MSTP which is based on RSTP according to the standard:

- ◆ **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
 - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
 - Short: Specifies 16-bit based values that range from 1-65535.
- ◆ **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

When the Switch Becomes Root

- ◆ **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
 - Default: 2
 - Minimum: 1
 - Maximum: The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$
- ◆ **Maximum Age** – 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. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
 - Default: 20
 - Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$
 - Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$
- ◆ **Forward Delay** – The maximum time (in seconds) this device 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 a discarding state; otherwise, temporary data loops might result.
 - Default: 15
 - Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$
 - Maximum: 30

RSTP does not depend on the forward delay timer in most cases. It is able to confirm that a port can transition to the forwarding state without having to rely on any timer configuration. To achieve fast convergence, RSTP relies on the use of edge ports, and automatic detection of point-to-point link types, both of which allow a port to directly transition to the forwarding state.

Configuration Settings for MSTP

- ◆ **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.
- ◆ **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- ◆ **Region Revision**⁷ – The revision for this MSTI. (Range: 0-65535; Default: 0)
- ◆ **Region Name**⁷ – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)
- ◆ **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

WEB INTERFACE

To configure global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes. Note that the parameters displayed for the spanning tree types (STP, RSTP, MSTP) varies as described in the preceding section.
5. Click Apply

7. The MST name and revision number are both required to uniquely identify an MST region.

Figure 106: Configuring Global Settings for STA (STP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status

☒ Enabled

Spanning Tree Type

STP

Priority (0-61440, in steps of 4096)

32768

BPDU Flooding

To VLAN

Advanced:

Path Cost Method

Long

Transmission Limit (1-10)

3

When the Switch Becomes Root:

Hello Time (1-10)

2

sec

Maximum Age (6-40)

20

sec

Forward Delay (4-30)

15

sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Apply

Revert

Figure 107: Configuring Global Settings for STA (RSTP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status

☒ Enabled

Spanning Tree Type

RSTP

Priority (0-61440, in steps of 4096)

32768

BPDU Flooding

To VLAN

Advanced:

Path Cost Method

Long

Transmission Limit (1-10)

3

When the Switch Becomes Root:

Hello Time (1-10)

2

sec

Maximum Age (6-40)

20

sec

Forward Delay (4-30)

15

sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Apply

Revert

Figure 108: Configuring Global Settings for STA (MSTP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status
☒ Enabled

Spanning Tree Type
MSTP

Priority (0-61440, in steps of 4096)
32768

BPDU Flooding
To VLAN

Advanced:

Path Cost Method
Long

Transmission Limit (1-10)
3

When the Switch Becomes Root:

Hello Time (1-10)
2 sec

Maximum Age (6-40)
20 sec

Forward Delay (4-30)
15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

MSTP Configuration

Max Instance Numbers
33

Configuration Digest
0xAC36177F50283CD4B83821D8AB26DE62

Region Revision (0-65535)
0

Region Name
00 00 e8 93 82 a0

Max Hop Count (1-40)
20

Apply Revert

DISPLAYING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Show Information) page to display a summary of the current bridge STA information that applies to the entire switch.

CLI REFERENCES

- ◆ ["show spanning-tree" on page 1084](#)
- ◆ ["show spanning-tree mst configuration" on page 1086](#)

PARAMETERS

The parameters displayed are described in the preceding section, except for the following items:

- ◆ **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).
- ◆ **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

- ◆ **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- ◆ **Root Path Cost** – The path cost from the root port on this switch to the root device.
- ◆ **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- ◆ **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

WEB INTERFACE

To display global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.

Figure 109: Displaying Global Settings for STA

Spanning Tree > STA

Step: 1. Configure Global Action: Show Information

Spanning Tree Information

Spanning Tree Status	Enabled	Spanning Tree Type	RSTP
Designated Root	32768.0000E89382A0	Bridge ID	32768.0000E89382A0
Root Port	0	Max Age	20 sec
Root Path Cost	0	Hello Time	2 sec
Configuration Changes	2	Forward Delay	15 sec
Last Topology Change	0 days, 3 hours, 51 minutes, 11 seconds		

CONFIGURING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Configure) page to configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

CLI REFERENCES

- ◆ ["Spanning Tree Commands" on page 1059](#)

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Spanning Tree** – Enables/disables STA on this interface.
(Default: Enabled)
- ◆ **BPDU Flooding** – Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled ([page 240](#)) or when spanning tree is disabled on a specific port. When flooding is 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 BPDU Flooding attribute ([page 240](#)). (Default: Enabled)
- ◆ **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
 - Default: 128
 - Range: 0-240, in steps of 16
- ◆ **Admin Path Cost** – This parameter is used by the STA 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 takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method⁸, 1-200,000,000 for the long path cost method)

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 12: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
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

8. Refer to ["Configuring Global Settings for STA" on page 240](#) for information on setting the path cost method.

Table 13: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (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

- ◆ **Admin Link Type** – The link type attached to this interface.
 - Point-to-Point – A connection to exactly one other bridge.
 - Shared – A connection to two or more bridges.
 - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- ◆ **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. 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. (Default: Disabled)
- ◆ **Admin Edge Port** – 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 timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Auto)
 - **Enabled** – Manually configures a port as an Edge Port.
 - **Disabled** – Disables the Edge Port setting.
 - **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages (see maximum age under ["Configuring Global Settings for STA" on page 240](#)).

An interface cannot function as an edge port under the following conditions:

- If spanning tree mode is set to STP ([page 240](#)), edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
 - If loopback detection is enabled ([page 238](#)) and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
 - If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
 - If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state (see "[Displaying Interface Settings for STA](#)" on [page 250](#)).
- ◆ **BPDU Guard** – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
 - ◆ **BPDU Filter** – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BPDU filtering is configured on a per-port basis. (Default: Disabled)
 - ◆ **Migration** – 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 Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

WEB INTERFACE

To configure interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes.
5. Click Apply.

Figure 110: Configuring Interface Settings for STA

The screenshot shows the 'Spanning Tree > STA' configuration page. At the top, there's a 'Step: 2. Configure Interface' and an 'Action: Configure' dropdown. Below this, there are radio buttons for 'Interface' (selected), 'Port', and 'Trunk'. A 'Port List' section shows 'Total: 28' ports. A table displays settings for 5 selected ports. The table has columns for Port, Spanning Tree, BPDU Flooding, Priority, Admin Path Cost, Admin Link Type, Root Guard, Admin Edge Port, BPDU Guard, BPDU Filter, and Migration. All 'Spanning Tree' and 'BPDU Flooding' settings are checked. 'Priority' is set to 128 and 'Admin Path Cost' to 0 for all ports. 'Admin Link Type' is set to 'Auto'. 'Root Guard' is enabled for all ports. 'Admin Edge Port' is set to 'Auto'. 'BPDU Guard' and 'BPDU Filter' are enabled for all ports. 'Migration' is enabled for all ports.

Port	Spanning Tree	BPDU Flooding	Priority (0-240, in steps of 16)	Admin Path Cost (0-2000000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Filter	Migration
1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input checked="" type="checkbox"/> Enabled	Auto	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
2	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input checked="" type="checkbox"/> Enabled	Auto	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input checked="" type="checkbox"/> Enabled	Auto	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input checked="" type="checkbox"/> Enabled	Auto	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	128	0	Auto	<input checked="" type="checkbox"/> Enabled	Auto	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

DISPLAYING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Show Information) page to display the current status of ports or trunks in the Spanning Tree.

CLI REFERENCES

- ◆ ["show spanning-tree" on page 1084](#)

PARAMETERS

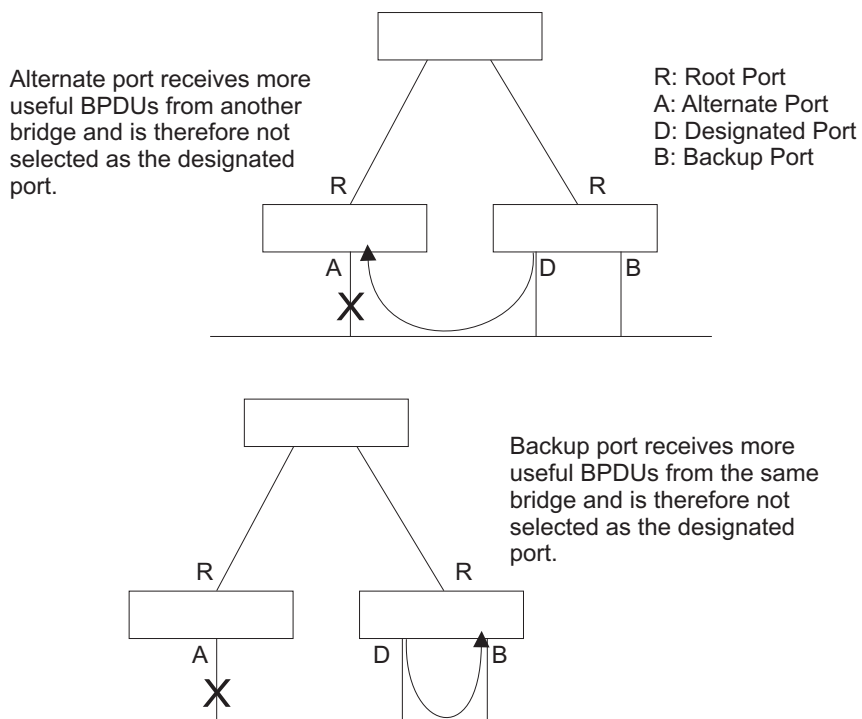
These parameters are displayed:

- ◆ **Spanning Tree** – Shows if STA has been enabled on this interface.
- ◆ **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.
- ◆ **STA Status** – Displays current state of this port within the Spanning Tree:
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
 - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
 - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- ◆ **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
 - ◆ **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
 - ◆ **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
 - ◆ **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
 - ◆ **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
 - ◆ **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on [page 246](#).
 - ◆ **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on [page 246](#) (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
 - ◆ **Port Role** – Roles are assigned according to whether the port is part of the active topology, that is the best port connecting a non-root bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), is the MSTI regional root (i.e., **master** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

Figure 111: STA Port Roles



WEB INTERFACE

To display interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 112: Displaying Interface Settings for STA

Spanning Tree > STA

Step: 2. Configure Interface Action: Show Information

Interface ☒ Port ☐ Trunk

Spanning Tree Port List Total: 28

Port	Spanning Tree	BPDU Flooding	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Enabled	Forwarding	3	0	32768.00000C0000FD	128.1	10000	Point-to-Point	Disabled	Designated
2	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.2	10000	Point-to-Point	Disabled	Disabled
3	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.5	10000	Point-to-Point	Disabled	Disabled

CONFIGURING MULTIPLE SPANNING TREES

Use the Spanning Tree > MSTP (Configure Global) page to create an MSTP instance, or to add VLAN groups to an MSTP instance.

CLI REFERENCES

- ◆ "Spanning Tree Commands" on page 1059

COMMAND USAGE

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 (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 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 240](#)) 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.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP ([page 240](#)).
2. Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP (Configure Global - Add) page.
3. Add the VLANs that will share this MSTI on the Spanning Tree > MSTP (Configure Global - Add Member) page.



NOTE: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

PARAMETERS

These parameters are displayed:

- ◆ **MST ID** – Instance identifier to configure. (Range: 0-4094)
- ◆ **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)
- ◆ **Priority** – The priority of 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: 32768)

WEB INTERFACE

To create instances for MSTP:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Specify the MST instance identifier and the initial VLAN member. Additional member can be added using the Spanning Tree > MSTP (Configure Global - Add Member) page. If the priority is not specified, the default value 32768 is used.
5. Click Apply.

Figure 113: Creating an MST Instance

The screenshot shows the 'Spanning Tree > MSTP' configuration page. At the top, there is a breadcrumb 'Spanning Tree > MSTP'. Below it, there are two dropdown menus: 'Step:' set to '1. Configure Global' and 'Action:' set to 'Add'. The main form area contains three input fields: 'MST ID (0-4094)' with the value '1', 'VLAN ID (1-4093)' with the value '1', and 'Priority (0-61440, in steps of 4096)' which is empty. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

To show the MSTP instances:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.

Figure 114: Displaying MST Instances

The screenshot shows the 'Spanning Tree > MSTP' configuration page with the 'Action:' dropdown set to 'Show'. Below the dropdowns, there is a table titled 'MST List' with a subtitle 'Total: 2'. The table has two columns: a checkbox column and an 'MST ID' column. There are two rows of data: one with MST ID '0' and one with MST ID '1'. At the bottom right, there are two buttons: 'Delete' and 'Revert'.

	MST ID
<input type="checkbox"/>	0
<input type="checkbox"/>	1

To modify the priority for an MST instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Modify from the Action list.
4. Modify the priority for an MSTP Instance.
5. Click Apply.

Figure 115: Modifying the Priority for an MST Instance

The screenshot shows the 'Spanning Tree > MSTP' configuration page. The 'Step' dropdown is set to '1. Configure Global' and the 'Action' dropdown is set to 'Modify'. Below this is the 'MST Details List' with a total of 2 items. The table has two columns: 'MST ID' and 'Priority (0-61440, in steps of 4096)'. The first row shows MST ID 0 with a priority of 0. The second row shows MST ID 1 with a priority of 32768. At the bottom of the table are 'Apply' and 'Revert' buttons.

MST ID	Priority (0-61440, in steps of 4096)
0	0
1	32768

To display global settings for MSTP:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.
4. Select an MST ID. The attributes displayed on this page are described under ["Displaying Global Settings for STA" on page 245](#).

Figure 116: Displaying Global Settings for an MST Instance

The screenshot shows the 'Spanning Tree > MSTP' configuration page. The 'Step' dropdown is set to '1. Configure Global' and the 'Action' dropdown is set to 'Show Information'. Below this is the 'MST ID' dropdown set to '1'. The table displays various attributes for MST ID 1:

Priority	0	Designated Root	32768.0030F1245660
Bridge ID	20	Root Port	2
Max Age	15 sec	Root Path Cost	32768.000001010010
Hello Time	23 sec	Configuration Changes	500000
Forward Delay	2 sec	Last Topology Change	0 days, 1 hours, 10 minutes, 0 seconds

To add additional VLAN groups to an MSTP instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Add Member from the Action list.
4. Select an MST instance from the MST ID list.
5. Enter the VLAN group to add to the instance in the VLAN ID field. Note that the specified member does not have to be a configured VLAN.
6. Click Apply

Figure 117: Adding a VLAN to an MST Instance

The screenshot shows the 'Spanning Tree > MSTP' configuration page. At the top, there is a breadcrumb 'Spanning Tree > MSTP'. Below it, there are two dropdown menus: 'Step: 1. Configure Global' and 'Action: Add Member'. Underneath, there is a section with two fields: 'MST ID' with a dropdown menu showing '1', and 'VLAN ID (1-4093)' with a text input field containing '2'. At the bottom right of this section, there are two buttons: 'Apply' and 'Revert'.

To show the VLAN members of an MSTP instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Member from the Action list.

Figure 118: Displaying Members of an MST Instance

The screenshot shows the 'Spanning Tree > MSTP' configuration page with the 'Action' set to 'Show Member'. The 'MST ID' dropdown is set to '0'. Below this, there is a 'Member List' section with a total of 4093 members. A pagination bar shows numbers 1 through 10, with '1' highlighted. Below the pagination bar is a table with two columns: a checkbox column and a 'VLAN' column. The table contains five rows, each with a checkbox and a VLAN number (1, 2, 3, 4, 5).

	VLAN
<input type="checkbox"/>	1
<input type="checkbox"/>	2
<input type="checkbox"/>	3
<input type="checkbox"/>	4
<input type="checkbox"/>	5

CONFIGURING INTERFACE SETTINGS FOR MSTP

Use the Spanning Tree > MSTP (Configure Interface - Configure) page to configure the STA interface settings for an MST instance.

CLI REFERENCES

- ◆ ["Spanning Tree Commands" on page 1059](#)

PARAMETERS

These parameters are displayed:

- ◆ **MST ID** – Instance identifier to configure. (Default: 0)
- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **STA Status** – Displays the current state of this interface within the Spanning Tree. (See ["Displaying Interface Settings for STA" on page 250](#) for additional information.)
 - **Discarding** – Port receives STA configuration messages, but does not forward packets.
 - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** – Port forwards packets, and continues learning addresses.
- ◆ **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)
- ◆ **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

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 recommended range is listed in [Table 12 on page 247](#).
The default path costs are listed in [Table 13 on page 248](#).

WEB INTERFACE

To configure MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Enter the priority and path cost for an interface
5. Click Apply.

Figure 119: Configuring MSTP Interface Settings

Spanning Tree > MSTP

Step: 2. Configure Interface Action: Configure

MST ID: 0

Interface: ☒ Port ☐ Trunk

Spanning Tree Port List Total: 28

Port	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
1	Forwarding	128	0
2	Discarding	128	0
3	Discarding	128	0
4	Discarding	128	0
5	Discarding	128	0

To display MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 120: Displaying MSTP Interface Settings

Spanning Tree > MSTP

Step: 2. Configure Interface Action: Show Information

MST ID: 0

Interface: ☒ Port ☐ Trunk

Spanning Tree Port List Total: 28

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Forwarding	6	0	0.0.00000C0000FD	128.1	10000	Point-to-Point	Disabled	Designated
2	Discarding	0	0	0.0.00000C0000FD	128.2	10000	Point-to-Point	Disabled	Disabled
3	Discarding	0	0	0.0.00000C0000FD	128.3	10000	Point-to-Point	Disabled	Disabled
4	Discarding	0	0	0.0.00000C0000FD	128.4	10000	Point-to-Point	Disabled	Disabled
5	Discarding	0	0	0.0.00000C0000FD	128.5	10000	Point-to-Point	Disabled	Disabled

The switch can set the maximum upload or download data transfer rate for any port. It can also 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.

Congestion Control includes following options:

- ◆ [Rate Limiting](#) – Sets the input and output rate limits for a port.
- ◆ [Storm Control](#) – Sets the traffic storm threshold for each interface.
- ◆ [Automatic Traffic Control](#) – Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

RATE LIMITING

Use the Traffic > Rate Limit page to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted 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, conforming traffic is forwarded without any changes.

CLI REFERENCES

- ◆ ["Rate Limit Commands" on page 1023](#)

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays the switch's ports or trunks.
- ◆ **Type** – Indicates the port type. (1000BASE-T, 1000BASE SFP⁹, 10GBASE SFP+)
- ◆ **Status** – Enables or disables the rate limit. (Default: Disabled)

9. ECS4510-28F

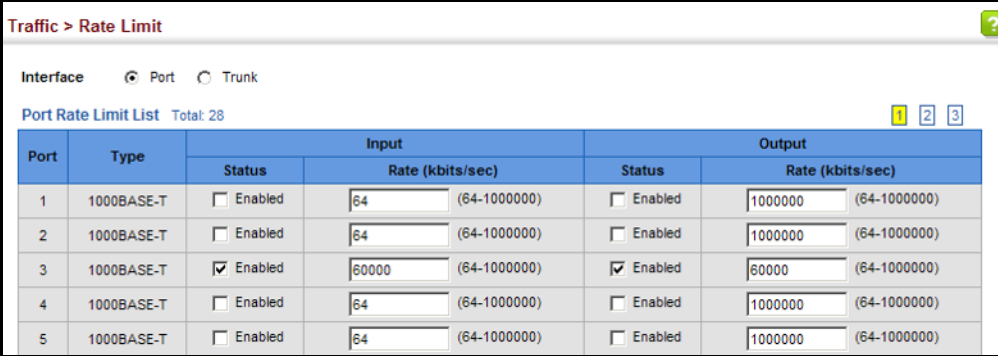
- ◆ **Rate** – Sets the rate limit level.
(Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports;
64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)

WEB INTERFACE

To configure rate limits:

1. Click Traffic, Rate Limit.
2. Set the interface type to Port or Trunk.
3. Enable the Rate Limit Status for the required interface.
4. Set the rate limit for the individual ports.
5. Click Apply.

Figure 121: Configuring Rate Limits



The screenshot shows the 'Traffic > Rate Limit' configuration page. At the top, there are radio buttons for 'Interface' type: 'Port' (selected) and 'Trunk'. Below this is a 'Port Rate Limit List' with a 'Total: 28' and three numbered tabs (1, 2, 3). The main table has columns for 'Port', 'Type', 'Input' (Status, Rate), and 'Output' (Status, Rate). The 'Input' and 'Output' sections each have a 'Status' checkbox and a 'Rate (kbits/sec)' field with a range in parentheses.

Port	Type	Input		Output	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	1000BASE-T	<input type="checkbox"/> Enabled	64 (64-1000000)	<input type="checkbox"/> Enabled	1000000 (64-1000000)
2	1000BASE-T	<input type="checkbox"/> Enabled	64 (64-1000000)	<input type="checkbox"/> Enabled	1000000 (64-1000000)
3	1000BASE-T	<input checked="" type="checkbox"/> Enabled	60000 (64-1000000)	<input checked="" type="checkbox"/> Enabled	60000 (64-1000000)
4	1000BASE-T	<input type="checkbox"/> Enabled	64 (64-1000000)	<input type="checkbox"/> Enabled	1000000 (64-1000000)
5	1000BASE-T	<input type="checkbox"/> Enabled	64 (64-1000000)	<input type="checkbox"/> Enabled	1000000 (64-1000000)

STORM CONTROL

Use the Traffic > Storm Control page 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.

CLI REFERENCES

- ◆ ["switchport packet-rate" on page 981](#)

COMMAND USAGE

- ◆ Broadcast Storm Control is enabled by default.

- ◆ 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.
- ◆ Traffic storms can be controlled at the hardware level using Storm Control or at the software level using [Automatic Traffic Control](#) which triggers various control responses. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.
- ◆ The rate limits set by this function are also used by automatic storm control when the control response is set to rate control on the Auto Traffic Control (Configure Interface) page.
- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 5000 Kbps, and the rate limit is set to 100000 Kbps on a Gigabit Ethernet port. Since 200000 Kbps is 1/5 of line speed, the received rate will actually be 1000 Kbps, or 1/5 of the 5000 Kbps limit set by the storm control command. It is therefore not advisable to use both of these features on the same interface.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Type** – Indicates interface type. (1000BASE-T, 1000BASE SFP¹⁰, 10GBASE SFP+)
- ◆ **Unknown Unicast** – Specifies storm control for unknown unicast traffic.
- ◆ **Multicast** – Specifies storm control for multicast traffic.
- ◆ **Broadcast** – Specifies storm control for broadcast traffic.
- ◆ **Status** – Enables or disables storm control. (Default: Enabled for broadcast storm control, disabled for multicast and unknown unicast storm control)
- ◆ **Rate** – Threshold level in kilobits per second.
(Range: 64-1,000,000 kbps for 1G ports, 64-10,000,000 kbps for 10G ports; Default: Disabled for unknown unicast and multicast traffic, 64 Kbps for broadcast traffic)

10. ECS4510-28F

WEB INTERFACE

To configure broadcast storm control:

1. Click Traffic, Storm Control.
2. Set the interface type to Port or Trunk.
3. Set the Status field to enable or disable storm control.
4. Set the required threshold beyond which the switch will start dropping packets.
5. Click Apply.

Figure 122: Configuring Storm Control

Traffic > Storm Control

Interface ☒ Port ☐ Trunk

Port Storm Control List Total: 28

Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (kbits/sec) (64-10000000)	Status	Rate (kbits/sec) (64-10000000)	Status	Rate (kbits/sec) (64-10000000)
1	1000BASE-T	<input type="checkbox"/> Enabled	64	<input type="checkbox"/> Enabled	64	<input checked="" type="checkbox"/> Enabled	64
2	1000BASE-T	<input type="checkbox"/> Enabled	64	<input type="checkbox"/> Enabled	64	<input checked="" type="checkbox"/> Enabled	64
3	1000BASE-T	<input checked="" type="checkbox"/> Enabled	60000	<input checked="" type="checkbox"/> Enabled	60000	<input checked="" type="checkbox"/> Enabled	60000
4	1000BASE-T	<input type="checkbox"/> Enabled	64	<input type="checkbox"/> Enabled	64	<input checked="" type="checkbox"/> Enabled	64
5	1000BASE-T	<input type="checkbox"/> Enabled	64	<input type="checkbox"/> Enabled	64	<input checked="" type="checkbox"/> Enabled	64

AUTOMATIC TRAFFIC CONTROL

Use the Traffic > Congestion Control > Auto Traffic Control pages to configure bounding thresholds for broadcast and multicast storms which can automatically trigger rate limits or shut down a port.

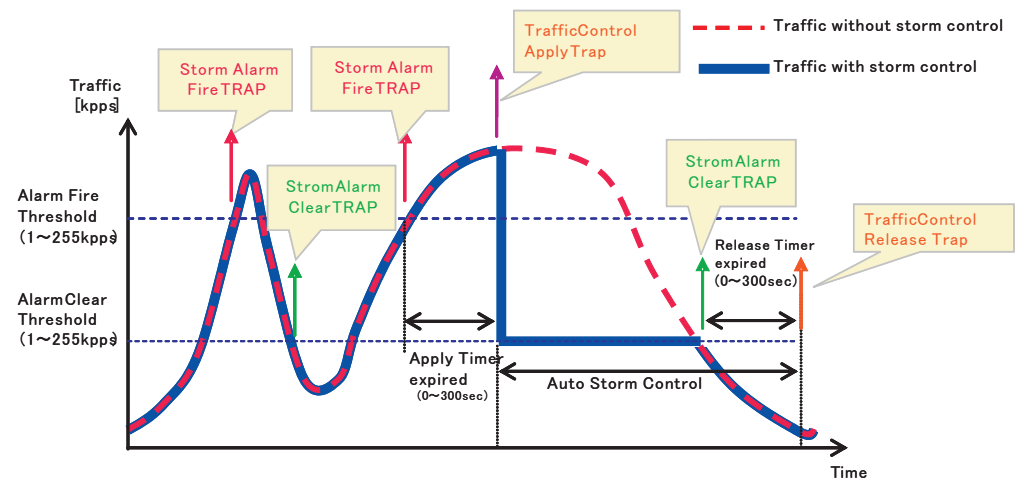
CLI REFERENCES

- ◆ "Automatic Traffic Control Commands" on page 1025

COMMAND USAGE

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Figure 123: Storm Control by Limiting the Traffic Rate

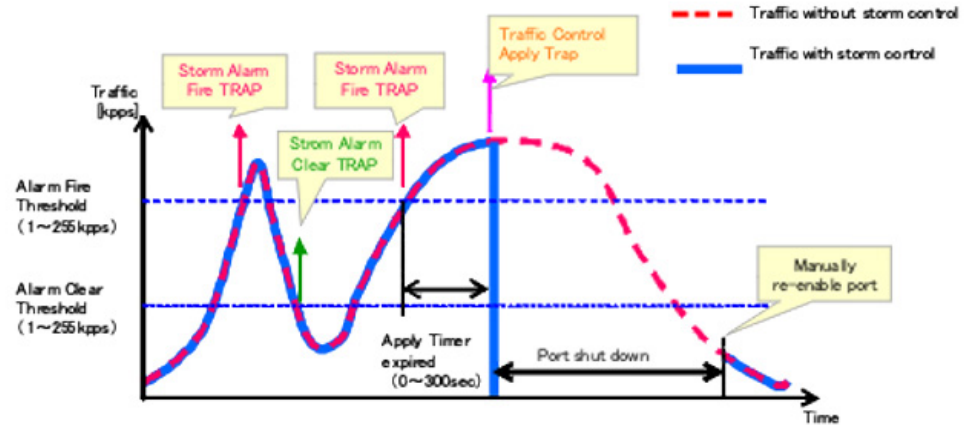


The key elements of this diagram are described below:

- ◆ Alarm Fire Threshold – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- ◆ When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- ◆ Alarm Clear Threshold – The lower threshold beneath which a control response can be automatically terminated after the release timer expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.
- ◆ When traffic falls below the alarm clear threshold after the release timer expires, traffic control (for rate limiting) will be stopped and a Traffic Control Release Trap sent and logged. Note that if the control action has shut down a port, it can only be manually re-enabled using Manual Control Release (see [page 266](#)).

- ◆ The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Figure 124: Storm Control by Shutting Down a Port



The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

Functional Limitations

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using Port Broadcast Control or Port Multicast Control (as described on [page 260](#)). However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

SETTING THE ATC TIMERS

Use the Traffic > Auto Traffic Control (Configure Global) page to set the time at which to apply the control response after ingress traffic has exceeded the upper threshold, and the time at which to release the control response after ingress traffic has fallen beneath the lower threshold.

CLI REFERENCES

- ◆ ["auto-traffic-control apply-timer"](#) on page 1028
- ◆ ["auto-traffic-control release-timer"](#) on page 1028

COMMAND USAGE

- ◆ After the apply timer expires, the settings in the Traffic > Automatic Traffic Control (Configure Interface) page are used to determine if a control action will be triggered (as configured under the Action field) or a trap message sent (as configured under the Trap Storm Fire field).
- ◆ The release timer only applies to a Rate Control response set in the Action field of the ATC (Interface Configuration) page. When a port has

been shut down by a control response, it must be manually re-enabled using the Manual Control Release (see [page 266](#)).

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Broadcast Apply Timer** – The interval after the upper threshold has been exceeded at which to apply the control response to broadcast storms. (Range: 1-300 seconds; Default: 300 seconds)
- ◆ **Broadcast Release Timer** – The time at which to release the control response after ingress traffic has fallen beneath the lower threshold for broadcast storms. (Range: 1-900 seconds; Default: 900 seconds)
- ◆ **Multicast Apply Timer** – The interval after the upper threshold has been exceeded at which to apply the control response to multicast storms. (Range: 1-300 seconds; Default: 300 seconds)
- ◆ **Multicast Release Timer** – The time at which to release the control response after ingress traffic has fallen beneath the lower threshold for multicast storms. (Range: 1-900 seconds; Default: 900 seconds)

WEB INTERFACE

To configure the response timers for automatic storm control:

1. Click Traffic, Automatic Traffic Control.
2. Select Configure Global from the Step field.
3. Set the apply and release timers for broadcast and multicast storms.
4. Click Apply.

Figure 125: Configuring ATC Timers

Traffic > Auto Traffic Control		
Step:	1. Configure Global	
Broadcast Apply Timer (1-300)	300	sec
Broadcast Release Timer (1-900)	900	sec
Multicast Apply Timer (1-300)	300	sec
Multicast Release Timer (1-900)	900	sec
<input type="button" value="Apply"/> <input type="button" value="Revert"/>		

CONFIGURING ATC THRESHOLDS AND RESPONSES

Use the Traffic > Auto Traffic Control (Configure Interface) page to set the storm control mode (broadcast or multicast), the traffic thresholds, the control response, to automatically release a response of rate limiting, or to send related SNMP trap messages.

CLI REFERENCES

- ◆ ["Automatic Traffic Control Commands" on page 1025](#)

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Storm Control** – Specifies automatic storm control for broadcast traffic or multicast traffic.
- ◆ **Port** – Port identifier.
- ◆ **State** – Enables automatic traffic control for broadcast or multicast storms. (Default: Disabled)

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the [Storm Control](#) menu. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

- ◆ **Action** – When the Alarm Fire Threshold (upper threshold) is exceeded and the apply timer expires, one of the following control responses will be triggered.
 - **Rate Control** – The rate of ingress traffic is limited to the level set by the Alarm Clear Threshold. Rate limiting is discontinued only after the traffic rate has fallen beneath the Alarm Clear Threshold (lower threshold), and the release timer has expired. (This is the default response.)
 - **Shutdown** – The port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled using the Manual Control Release attribute.
- ◆ **Auto Release Control** – Automatically stops a traffic control response of rate limiting when traffic falls below the alarm clear threshold and the release timer expires as illustrated in [Figure 123 on page 263](#). When traffic control stops, the event is logged by the system and a Traffic Release Trap can be sent. (Default: Disabled)

If automatic control release is not enabled and a control response of rate limiting has been triggered, you can manually stop the rate limiting response using the Manual Control Release attribute. If the control response has shut down a port, it can also be re-enabled using Manual Control Release.
- ◆ **Alarm Fire Threshold** – The upper threshold for ingress traffic beyond which a storm control response is triggered after the Apply Timer expires. (Range: 1-255 kilo-packets per second; Default: 128 Kpps)

Once the traffic rate exceeds the upper threshold and the Apply Timer expires, a trap message will be sent if configured by the Trap Storm Fire attribute.

- ◆ **Alarm Clear Threshold** – The lower threshold for ingress traffic beneath which a control response for rate limiting will be released after the Release Timer expires, if so configured by the Auto Release Control attribute. (Range: 1-255 kilo-packets per second; Default: 128 Kpps)

If rate limiting has been configured as a control response and Auto Control Release is enabled, rate limiting will be discontinued after the traffic rate has fallen beneath the lower threshold, and the Release Timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using Manual Control Release.

Once the traffic rate falls beneath the lower threshold and the Release Timer expires, a trap message will be sent if configured by the Trap Storm Clear attribute.

- ◆ **Trap Storm Fire** – Sends a trap when traffic exceeds the upper threshold for automatic storm control. (Default: Disabled)
- ◆ **Trap Storm Clear** – Sends a trap when traffic falls beneath the lower threshold after a storm control response has been triggered. (Default: Disabled)
- ◆ **Trap Traffic Apply** – Sends a trap when traffic exceeds the upper threshold for automatic storm control and the apply timer expires. (Default: Disabled)
- ◆ **Trap Traffic Release** – Sends a trap when traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. (Default: Disabled)
- ◆ **Manual Control Release** – Manually releases a control response of rate-limiting or port shutdown any time after the specified action has been triggered.

If this function is enabled for any port, clicking Apply with manually release the control response, and clear the check box.

WEB INTERFACE

To configure the response timers for automatic storm control:

1. Click Traffic, Automatic Traffic Control.
2. Select Configure Interface from the Step field.
3. Enable or disable ATC as required, set the control response, specify whether or not to automatically release the control response of rate limiting, set the upper and lower thresholds, and specify which trap messages to send.
4. Click Apply.

Figure 126: Configuring ATC Interface Attributes

Traffic > Auto Traffic Control

Step: 2. Configure Interface

Storm Control
☒ Broadcast
☐ Multicast

Auto Traffic Control Broadcast List Total: 28

Port	State	Action	Auto Release Control	Alarm Fire Threshold (1-255 kpps)	Alarm Clear Threshold (1-255 kpps)	Trap Storm Fire	Trap Storm Clear	Trap Traffic Apply	Trap Traffic Release	Manual Control Release
1	<input type="checkbox"/> Enabled	Rate Control	<input type="checkbox"/> Enabled	128	128	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled	Rate Control	<input type="checkbox"/> Enabled	128	128	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled	Rate Control	<input type="checkbox"/> Enabled	128	128	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled	Rate Control	<input type="checkbox"/> Enabled	128	128	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled	Rate Control	<input type="checkbox"/> Enabled	128	128	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

Class of Service (CoS) allows 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. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

This chapter describes the following basic topics:

- ◆ [Layer 2 Queue Settings](#) – Configures each queue, including the default priority, queue mode, queue weight, and mapping of packets to queues based on CoS tags.
- ◆ [Layer 3/4 Priority Settings](#) – Selects the method by which inbound packets are processed (DSCP or CoS), and sets the per-hop behavior and drop precedence for internal processing.

LAYER 2 QUEUE SETTINGS

This section describes how to configure the default priority for untagged frames, set the queue mode, set the weights assigned to each queue, and map class of service tags to queues.

SETTING THE DEFAULT PRIORITY FOR INTERFACES

Use the Traffic > Priority > Default Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

CLI REFERENCES

- ◆ ["switchport priority default" on page 1170](#)

COMMAND USAGE

- ◆ This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage, but can be configured to process each queue in strict order, or use a combination of strict and weighted queueing.
- ◆ 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.

- ◆ If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Default Priority.
2. Select the interface type to display (Port or Trunk).
3. Modify the default priority for any interface.
4. Click Apply.

Figure 127: Setting the Default Port Priority

Port	CoS (0-7)
1	0
2	0
3	5
4	0
5	0

SELECTING THE QUEUE MODE

Use the Traffic > Priority > Queue page to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue. It can also be configured to use a combination of strict and weighted queuing.

CLI REFERENCES

- ◆ ["queue mode" on page 1168](#)
- ◆ ["show queue mode" on page 1171](#)

COMMAND USAGE

- ◆ Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- ◆ WRR queuing specifies a relative weight for each queue. 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.
- ◆ If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field 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 one of the queuing modes that use a combination of strict and weighted queuing.

- ◆ The specified queue mode applies to all interfaces.
- ◆ Protocols used to synchronize distributed switches use packets of 1588 bytes to control the synchronization process. This switch therefore assigns packets of this size to the highest priority queue to ensure quick passage.

PARAMETERS

These parameters are displayed:

- ◆ **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, and servicing each queue in a round-robin fashion. (This is the default setting.)
 - **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the remaining queues.
- ◆ **Queue ID** – The ID of the priority queue. (Range: 0-7)
- ◆ **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict service is used for the high priority queues and

weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority. (Default: Disabled)

- ◆ **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6, 8, 10, 12 and 14 are assigned to queues 0 - 7 respectively)

WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Queue.
2. Set the queue mode.
3. If the weighted queue mode is selected, the queue weight can be modified if required.
4. If the queue mode that uses a combination of strict and weighted queueing is selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.
5. Click Apply.

Figure 128: Setting the Queue Mode (Strict)

The screenshot shows the 'Traffic > Priority > Queue' configuration page. The 'Queue Mode' is set to 'Strict' in a dropdown menu. Below the dropdown are 'Apply' and 'Revert' buttons.

Figure 129: Setting the Queue Mode (WRR)

The screenshot shows the 'Traffic > Priority > Queue' configuration page with the 'Queue Mode' set to 'WRR'. Below the dropdown is a 'Queue Setting Table' with 8 columns: Queue ID and Weight (1-255). The table contains 8 rows, each with a Queue ID from 0 to 7 and a corresponding weight value. Below the table are 'Apply' and 'Revert' buttons.

Queue ID	Weight (1-255)
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Figure 130: Setting the Queue Mode (Strict and WRR)

Traffic > Priority > Queue

Queue Mode: Strict and WRR

Queue Setting Table Total: 8

Queue ID	Strict Mode	Weight (1-255)
0	Disabled	1
1	Disabled	2
2	Disabled	4
3	Disabled	6
4	Disabled	8
5	Disabled	10
6	Disabled	12
7	Disabled	14

Apply Revert

MAPPING COS VALUES TO EGRESS QUEUES

Use the Traffic > Priority > PHB to Queue page to specify the hardware output queues to use based on the internal per-hop behavior value. (For more information on exact manner in which the ingress priority tags are mapped to egress queues for internal processing, see ["Mapping CoS Priorities to Internal DSCP Values"](#) on page 280).

The switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in [Table 14](#). The following table indicates the default mapping of internal per-hop behavior to the hardware queues. The actual mapping may differ if the CoS priorities to internal DSCP values have been modified ([page 280](#)).

Table 14: IEEE 802.1p Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in [Table 15](#). However, priority levels can be mapped to the switch's output queues in any way that benefits application traffic for the network.

Table 15: CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort

Table 15: CoS Priority Levels (Continued)

Priority Level	Traffic Type
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

CLI REFERENCES

- ◆ ["qos map phb-queue" on page 1175](#)

COMMAND USAGE

- ◆ Egress packets are placed into the hardware queues according to the mapping defined by this command.
- ◆ The default internal PHB to output queue mapping is shown below.

Table 16: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	2	0	1	3	4	5	6	7

- ◆ The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Specifies a port.
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7, where 7 is the highest priority)
- ◆ **Queue** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

WEB INTERFACE

To map internal PHB to hardware queues:

1. Click Traffic, Priority, PHB to Queue.
2. Select Configure from the Action list.
3. Select a port.
4. Map an internal PHB to a hardware queue. Depending on how an ingress packet is processed internally based on its CoS value, and the assigned output queue, the mapping done on this page can effectively determine the service priority for different traffic classes.
5. Click Apply.

Figure 131: Mapping CoS Values to Egress Queues

Traffic > Priority > PHB to Queue

Action: Configure

Port: 1

PHB (0-7):

Queue (0-7):

Apply Revert

To show the internal PHB to hardware queue map:

1. Click Traffic, Priority, PHB to Queue.
2. Select Show from the Action list.
3. Select an interface.

Figure 132: Showing CoS Values to Egress Queue Mapping

Traffic > Priority > PHB to Queue

Action: Show

Port: 1

PHB to Queue Mapping List Total: 8

PHB	Queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

LAYER 3/4 PRIORITY SETTINGS

Mapping Layer 3/4 Priorities to CoS Values

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet, or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner – The precedence for priority mapping is DSCP Priority and then Default Port Priority.



NOTE: The default settings used for mapping priority values from ingress traffic to internal DSCP values are used to determine the hardware queues used for egress traffic, not to replace the priority values. These defaults 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.

SETTING PRIORITY PROCESSING TO DSCP OR CoS

The switch allows a choice between using DSCP or CoS priority processing methods. Use the Priority > Trust Mode page to select the required processing method.

CLI REFERENCES

- ◆ ["qos map trust-mode" on page 1176](#)

COMMAND USAGE

- ◆ If the QoS mapping mode is set to DSCP, 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 269](#)) is used for priority processing.
- ◆ If the QoS mapping mode is set to CoS, 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 269](#)) is used for priority processing.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Trust Mode**
 - **CoS** – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)
 - **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.

WEB INTERFACE

To configure the trust mode:

1. Click Traffic, Priority, Trust Mode.
2. Set the trust mode for any port.
3. Click Apply.

Figure 133: Setting the Trust Mode

Port	Trust Mode
1	DSCP
2	CoS
3	CoS
4	CoS
5	CoS

MAPPING INGRESS DSCP VALUES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > DSCP to DSCP page to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

CLI REFERENCES

- ◆ ["qos map dscp-mutation" on page 1174](#)

COMMAND USAGE

- ◆ Enter per-hop behavior and drop precedence for any of the DSCP values 0 - 63.

- ◆ This map is only used when the priority mapping mode is set to DSCP (see [page 276](#)), and the ingress packet type is IPv4. Any attempt to configure the DSCP mutation map will not be accepted by the switch, unless the trust mode has been set to DSCP.
- ◆ Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Specifies a port.
- ◆ **DSCP** – DSCP value in ingress packets. (Range: 0-63)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 17: Default Mapping of DSCP Values to Internal PHB/Drop Values

	ingress-dscp1	0	1	2	3	4	5	6	7	8	9
ingress-dscp10											
0		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 internal-dscp is shown at the intersecting cell in the table.

The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

WEB INTERFACE

To map DSCP values to internal PHB/drop precedence:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Configure from the Action list.
3. Select a port.

4. Set the PHB and drop precedence for any DSCP value.
5. Click Apply.

Figure 134: Configuring DSCP to DSCP Internal Mapping

Traffic > Priority > DSCP to DSCP

Action: Configure

Port: 1

DSCP (0-63): 1

PHB (0-7): 3

Drop Precedence: 1: Red

Apply Revert

To show the DSCP to internal PHB/drop precedence map:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Show from the Action list.
3. Select a port.

Figure 135: Showing DSCP to DSCP Internal Mapping

Traffic > Priority > DSCP to DSCP

Action: Show

Port: 1

DSCP to DSCP Mapping List Total: 64

	DSCP	PHB	Drop Precedence
<input type="checkbox"/>	0	0	0
<input type="checkbox"/>	1	0	1
<input type="checkbox"/>	2	0	0
<input type="checkbox"/>	3	0	3
<input type="checkbox"/>	4	0	0
<input type="checkbox"/>	5	0	1
<input type="checkbox"/>	6	0	0
<input type="checkbox"/>	7	0	3
<input type="checkbox"/>	8	1	0
<input type="checkbox"/>	9	1	1

Default Revert

MAPPING CoS PRIORITIES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > CoS to DSCP page to map CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

CLI REFERENCES

- ◆ "qos map cos-dscp" on page 1172

COMMAND USAGE

- ◆ The default mapping of CoS to PHB values is shown in [Table 18 on page 281](#).
- ◆ Enter up to eight CoS/CFI paired values, per-hop behavior and drop precedence.
- ◆ If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- ◆ The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used to control traffic congestion.
- ◆ The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Specifies a port.
- ◆ **CoS** – CoS value in ingress packets. (Range: 0-7)
- ◆ **CFI** – Canonical Format Indicator. Set to this parameter to "0" to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 18: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS	CFI	0	1
0		(0,0)	(0,0)
1		(1,0)	(1,0)
2		(2,0)	(2,0)
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)

WEB INTERFACE

To map CoS/CFI values to internal PHB/drop precedence:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Configure from the Action list.
3. Select a port.
4. Set the PHB and drop precedence for any of the CoS/CFI combinations.
5. Click Apply.

Figure 136: Configuring CoS to DSCP Internal Mapping

Traffic > Priority > CoS to DSCP

Action: Configure

Port 1

CoS (0-7) 0

CFI (0-1) 1

PHB (0-7) 0

Drop Precedence 0: Green

Apply Revert

To show the CoS/CFI to internal PHB/drop precedence map:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Show from the Action list.
3. Select a port.

Figure 137: Showing CoS to DSCP Internal Mapping

Traffic > Priority > CoS to DSCP

Action: Show

Port 1

CoS to DSCP Mapping List Total: 16

<input type="checkbox"/>	CoS	CFI	PHB	Drop Precedence
<input type="checkbox"/>	0	0	0	0
<input type="checkbox"/>	0	1	0	0
<input type="checkbox"/>	1	0	1	0
<input type="checkbox"/>	1	1	1	0
<input type="checkbox"/>	2	0	2	0
<input type="checkbox"/>	2	1	2	0
<input type="checkbox"/>	3	0	3	0
<input type="checkbox"/>	3	1	3	0
<input type="checkbox"/>	4	0	4	0
<input type="checkbox"/>	4	1	4	0

Default Revert

This chapter describes the following tasks required to apply QoS policies:

Class Map – Creates a map which identifies a specific class of traffic.

Policy Map – Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic.

Binding to a Port – Applies a policy map to an ingress port.

OVERVIEW

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists, CoS values or source ports. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.



NOTE: You can configure up to 16 rules per class map. You can also include multiple classes in a policy map.

NOTE: You should create a class map before creating a policy map. Otherwise, you will not be able to select a class map from the policy rule settings screen (see [page 287](#)).

COMMAND USAGE

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the Configure Class (Add) page to designate a class name for a specific category of traffic.
2. Use the Configure Class (Add Rule) page to edit the rules for each class which specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN, a CoS value, or a source port.
3. Use the Configure Policy (Add) page to designate a policy name for a specific manner in which ingress traffic will be handled.
4. Use the Configure Policy (Add Rule) page to add one or more classes to the policy map. Assign policy rules to each class by "setting" the QoS value (CoS or PHB) to be assigned to the matching traffic class. The policy rule can also be configured to monitor the maximum throughput and burst rate. Then specify the action to take for conforming traffic, or the action to take for a policy violation.
5. Use the Configure Interface page to assign a policy map to a specific interface.

CONFIGURING A CLASS MAP

A class map is used for matching packets to a specified class. Use the Traffic > DiffServ (Configure Class) page to configure a class map.

CLI REFERENCES

- ◆ ["Quality of Service Commands" on page 1181](#)

COMMAND USAGE

- ◆ The class map is used with a policy map ([page 287](#)) to create a service policy ([page 297](#)) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.
- ◆ Up to 32 class maps can be configured.

PARAMETERS

These parameters are displayed:

Add

- ◆ **Class Name** – Name of the class map. (Range: 1-32 characters)
- ◆ **Type** – The criteria specified by the match command.
 - **Match All** – Match all conditions within a class map.
 - **Match Any** – Match any condition within a class map.

- ◆ **Description** – A brief description of a class map. (Range: 1-64 characters)

Add Rule

- ◆ **Class Name** – Name of the class map.
- ◆ **Type** – The criteria specified by the match command. (This field is set on the Add page.)
- ◆ **ACL** – Name of an access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 ACLs and MAC ACLs.
- ◆ **IP DSCP** – A DSCP value. (Range: 0-63)
- ◆ **IP Precedence** – An IP Precedence value. (Range: 0-7)
- ◆ **IPv6 DSCP** – A DSCP value contained in an IPv6 packet. (Range: 0-63)
- ◆ **VLAN ID** – A VLAN. (Range: 1-4093)
- ◆ **CoS** – A CoS value. (Range: 0-7)
- ◆ **Source Port** – A source port. (Range: 1-28/52)

WEB INTERFACE

To configure a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add from the Action list.
4. Enter a class name.
5. Set the Type to match any rule or all rules.
6. Enter a description.
7. Click Add.

Figure 138: Configuring a Class Map

The screenshot shows a web interface for configuring a class map. At the top, it says "Traffic > DiffServ". Below this, there are two dropdown menus: "Step:" with "1. Configure Class" selected, and "Action:" with "Add" selected. The main configuration area has three fields: "Class Name" with the value "rd-class", "Type" with a dropdown menu showing "Match Any", and "Description" with the value "class for software group". At the bottom right, there are two buttons: "Apply" and "Revert".

To show the configured class maps:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show from the Action list.

Figure 139: Showing Class Maps

Traffic > DiffServ

Step: 1. Configure Class Action: Show

Class List Total: 1

<input type="checkbox"/>	Class Name	Type	Description
<input type="checkbox"/>	rd-class	Match Any	class for sotware group

Delete Revert

To edit the rules for a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of a class map.
5. Specify type of traffic for this class based on an access list, DSCP or IP Precedence value, VLAN, CoS value, or source port. You can specify up to 16 items to match when assigning ingress traffic to a class map.
6. Click Apply.

Figure 140: Adding Rules to a Class Map

Traffic > DiffServ

Step: 1. Configure Class Action: Add Rule

Class Name: rd-class

Type: Match Any

Rule:

☐ ACL

☒ IP DSCP (0-63)

☐ IP Precedence (0-7)

☐ IPv6 DSCP (0-63)

☐ VLAN ID (1-4093)

☐ CoS (0-7)

☐ Source Port

Apply Revert

To show the rules for a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show Rule from the Action list.

Figure 141: Showing the Rules for a Class Map

The screenshot shows the 'Traffic > DiffServ' configuration page. At the top, there's a breadcrumb 'Traffic > DiffServ'. Below it, the 'Step:' dropdown is set to '1. Configure Class' and the 'Action:' dropdown is set to 'Show Rule'. Under 'Class Name', 'rd-class' is selected. The 'Type' is 'Match Any'. Below this, there's a 'Rule List' section with a 'Total: 2' count. The list contains two rules: 'IP DSCP 3' and 'IP Precedence 3'. Each rule has a checkbox to its left. At the bottom right, there are 'Delete' and 'Revert' buttons.

Rule
IP DSCP 3
IP Precedence 3

CREATING QOS POLICIES

Use the Traffic > DiffServ (Configure Policy) page to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements ([page 284](#)), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces ([page 297](#)).

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps.

The class of service or per-hop behavior (i.e., the priority used for internal queue processing) can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to conforming and non-conforming traffic based by one of three distinct policing methods as described below.

Police Flow Meter – Defines the committed information rate (maximum throughput), committed burst size (burst rate), and the action to take for conforming and non-conforming traffic.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the "burst" field (BC), and the average rate tokens are removed from the bucket is specified by the "rate" option (CIR). Action may be taken for traffic conforming to the maximum throughput, or exceeding the maximum throughput.

srTCM Police Meter – Defines an enforcer for classified traffic based on a single rate three color meter scheme defined in RFC 2697. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and excess burst size (BE). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the excess burst size.

- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet. A packet is marked green if it doesn't exceed the committed information rate and committed burst size, yellow if it does exceed the committed information rate and committed burst size, but not the excess burst size, and red otherwise.
- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

The token buckets C and E are initially full, that is, the token count $T_c(0) = BC$ and the token count $T_e(0) = BE$. Thereafter, the token counts T_c and T_e are updated CIR times per second as follows:

- If T_c is less than BC, T_c is incremented by one, else
- if T_e is less then BE, T_e is incremented by one, else
- neither T_c nor T_e is incremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Blind mode:

- 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

- if $Te(t) - B \geq 0$, the packet is yellow and Te is decremented by B down to the minimum value of 0,
- else the packet is red and neither Tc nor Te is decremented.

When a packet of size B bytes arrives at time t , the following happens if srTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as green and $Tc(t) - B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if $Te(t) - B \geq 0$, the packet is yellow and Te is decremented by B down to the minimum value of 0, else
- the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

trTCM Police Meter – Defines an enforcer for classified traffic based on a two rate three color meter scheme defined in RFC 2698. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate), and peak burst size (BP). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the peak burst size.

- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, P and C , which are based on the rates PIR and CIR,

respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.

The token buckets P and C are initially (at time 0) full, that is, the token count $Tp(0) = BP$ and the token count $Tc(0) = BC$. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Blind mode:

- If $Tp(t) - B < 0$, the packet is red, else
- if $Tc(t) - B < 0$, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as red or if $Tp(t) - B < 0$, the packet is red, else
 - if the packet has been precolored as yellow or if $Tc(t) - B < 0$, the packet is yellow and Tp is decremented by B, else
 - the packet is green and both Tp and Tc are decremented by B.
- ◆ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

CLI REFERENCES

- ◆ ["Quality of Service Commands" on page 1181](#)

COMMAND USAGE

- ◆ A policy map can contain 512 class statements that can be applied to the same interface ([page 297](#)). Up to 32 policy maps can be configured for ingress ports.
- ◆ After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy ([page 297](#)) to take effect.

PARAMETERS

These parameters are displayed:

Add

- ◆ **Policy Name** – Name of policy map. (Range: 1-32 characters)
- ◆ **Description** – A brief description of a policy map. (Range: 1-256 characters)

Add Rule

- ◆ **Policy Name** – Name of policy map.
- ◆ **Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.
- ◆ **Action** – This attribute is used to set an internal QoS value in hardware for matching packets. The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.
 - **Set CoS** – Configures the service provided to ingress traffic by setting an internal CoS value for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

See [Table 18, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence," on page 281](#)).
 - **Set PHB** – Configures the service provided to ingress traffic by setting the internal per-hop behavior for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

See [Table 17, "Default Mapping of DSCP Values to Internal PHB/Drop Values," on page 278](#)).
 - **Set IP DSCP** – Configures the service provided to ingress traffic by setting an IP DSCP value for a matching packet (as specified in rule settings for a class map). (Range: 0-63)
- ◆ **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
- ◆ **Meter Mode** – Selects one of the following policing methods.
 - **Flow** (Police Flow) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and the action to take for conforming and non-conforming traffic. Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the "burst" field, and the average rate tokens are removed from the bucket is by specified by the "rate" option.
 - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

The rate cannot exceed the configured interface speed.
 - **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.
 - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.
- **Violate** – Specifies whether the traffic that exceeds the maximum rate (CIR) will be dropped or the DSCP service level will be reduced.
 - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
 - **Drop** – Drops out of conformance traffic.
- **srTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate) and excess burst size (BE), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the excess burst size, or exceeding the excess burst size. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet.

The color modes include “Color-Blind” which assumes that the packet stream is uncolored, and “Color-Aware” which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under “srTCM Police Meter.”

- **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)
The rate cannot exceed the configured interface speed.
- **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-16000000 at a granularity of 4k bytes)
The burst size cannot exceed 16 Mbytes.
- **Excess Burst Size** (BE) – Burst in excess of committed burst size. (Range: 64-16000000 at a granularity of 4k bytes)
The burst size cannot exceed 16 Mbytes.
- **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.
 - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.
 - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
 - **Drop** – Drops out of conformance traffic.
- **Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.
 - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
 - **Drop** – Drops out of conformance traffic.
- **trTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate) and peak burst size (BP), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the peak information rate, or exceeding the peak information rate. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet.

The color modes include “Color-Blind” which assumes that the packet stream is uncolored, and “Color-Aware” which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under “trTCM Police Meter.”

- **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)
The rate cannot exceed the configured interface speed.
- **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-16000000 at a granularity of 4k bytes)
The burst size cannot exceed 16 Mbytes.
- **Peak Information Rate** (PIR) – Rate in kilobits per second. (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)
The rate cannot exceed the configured interface speed.
- **Peak Burst Size** (BP) – Burst size in bytes. (Range: 64-16000000 at a granularity of 4k bytes)
The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.
- **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.
- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.
- **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
- **Drop** – Drops out of conformance traffic.
- **Violate** – Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.
- **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
- **Drop** – Drops out of conformance traffic.

WEB INTERFACE

To configure a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Add from the Action list.
4. Enter a policy name.
5. Enter a description.
6. Click Add.

Figure 142: Configuring a Policy Map

The screenshot shows a web interface for configuring a policy map. At the top, it says "Traffic > DiffServ". Below that, there are two dropdown menus: "Step:" with "2. Configure Policy" selected, and "Action:" with "Add" selected. Below these are two text input fields: "Policy Name" with the value "rd-policy" and "Description" with the value "for the software group". At the bottom right, there are two buttons: "Apply" and "Revert".

To show the configured policy maps:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Show from the Action list.

Figure 143: Showing Policy Maps

The screenshot shows a web interface for configuring DiffServ policies. At the top, it says "Traffic > DiffServ". Below this, there are two dropdown menus: "Step:" with "2. Configure Policy" selected, and "Action:" with "Show" selected. Below these is a section titled "Policy List Total: 1". It contains a table with two columns: "Policy Name" and "Description". There is one row in the table with the policy name "rd-policy" and the description "for the software group". To the left of the table, there are two checkboxes, both of which are unchecked. At the bottom right of the table, there are two buttons: "Delete" and "Revert".

	Policy Name	Description
<input type="checkbox"/>	rd-policy	for the software group

To edit the rules for a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of a policy map.
5. Set the CoS or per-hop behavior for matching packets to specify the quality of service to be assigned to the matching traffic class. Use one of the metering options to define parameters such as the maximum throughput and burst rate. Then specify the action to take for conforming traffic, the action to tack for traffic in excess of the maximum rate but within the peak information rate, or the action to take for a policy violation.
6. Click Apply.

Figure 144: Adding Rules to a Policy Map

Traffic > DiffServ

Step: 2. Configure Policy Action: Add Rule

Policy Name: rd-policy

Rule:

Class Name: rd-class

☒ Action: Set CoS (0-7) 3

☒ Meter

Meter Mode: Flow

Committed Information Rate (0-10000000): 10000000 kbps

Committed Burst Size (64-16000000): 4000 bytes

Excess Burst Size (64-16000000): bytes

Peak Information Rate (0-10000000): kbps

Peak Burst Size (64-16000000): bytes

Conform: Transmit

Exceed: Set IP DSCP (0-63)

Violate: Drop

To show the rules for a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Show Rule from the Action list.

Figure 145: Showing the Rules for a Policy Map

Traffic > DiffServ

Step: 2. Configure Policy Action: Show Rule

Policy Name: rd-policy

Rule List Total: 1

	Class Name	Action	Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Exceeded Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)	Conform	Exceed	Violate
<input type="checkbox"/>	rd-class	Set PHB 3	Flow	1000000	4000				Transmit		Drop

Delete Revert

ATTACHING A POLICY MAP TO A PORT

Use the Traffic > DiffServ (Configure Interface) page to bind a policy map to a port.

CLI REFERENCES

- ◆ ["Quality of Service Commands" on page 1181](#)

COMMAND USAGE

First define a class map, define a policy map, and then bind the service policy to the required interface.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Specifies a port.
- ◆ **Ingress** – Applies the selected rule to ingress traffic.
- ◆ **Egress** – Applies the selected rule to egress traffic.

WEB INTERFACE

To bind a policy map to a port:

1. Click Traffic, DiffServ.
2. Select Configure Interface from the Step list.
3. Check the box under the Ingress field to enable a policy map for a port.
4. Select a policy map from the scroll-down box.
5. Click Apply.

Figure 146: Attaching a Policy Map to a Port

Traffic > DiffServ

Step: 3. Configure Interface

Port Service Policy List Total: 28

Port	Ingress	Egress
1	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
2	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
3	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
4	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
5	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
6	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
7	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
8	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
9	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy
10	<input type="checkbox"/> rd-policy	<input type="checkbox"/> rd-policy

Apply Revert

This chapter covers the following topics:

- ◆ [Global Settings](#) – Enables VOIP globally, sets the Voice VLAN, and the aging time for attached ports.
- ◆ [Telephony OUI List](#) – Configures the list of phones to be treated as VOIP devices based on the specified Organization Unit Identifier (OUI).
- ◆ [Port Settings](#) – Configures the way in which a port is added to the Voice VLAN, the filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to voice traffic.

OVERVIEW

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 can provide higher voice quality by preventing excessive packet delays, packet loss, and jitter. This is best achieved by assigning all VoIP traffic to a single Voice VLAN.

The use of a Voice VLAN has several advantages. It provides security by isolating the VoIP traffic from other data traffic. End-to-end QoS policies and high priority can be applied to VoIP VLAN traffic across the network, guaranteeing the bandwidth it needs. VLAN isolation also protects against disruptive broadcast and multicast traffic that can seriously affect voice quality.

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. The 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 the Voice VLAN. Alternatively, switch ports can be manually configured.

CONFIGURING VOIP TRAFFIC

Use the Traffic > VoIP (Configure Global) page to configure the switch for VoIP traffic. First enable automatic detection of VoIP devices attached to the switch ports, then set the Voice VLAN ID for the network. The Voice VLAN aging time can also be set to remove a port from the Voice VLAN when VoIP traffic is no longer received on the port.

CLI REFERENCES

- ◆ ["Configuring Voice VLANs" on page 1160](#)

COMMAND USAGE

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), first ensure that VLAN membership is not set to access mode (see ["Adding Static Members to VLANs" on page 199](#)).

PARAMETERS

These parameters are displayed:

- ◆ **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- ◆ **Voice VLAN** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4093)
- ◆ **Voice VLAN Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)



NOTE: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

WEB INTERFACE

To configure global settings for a Voice VLAN:

1. Click Traffic, VoIP.
2. Select Configure Global from the Step list.
3. Enable Auto Detection.
4. Specify the Voice VLAN ID.
5. Adjust the Voice VLAN Aging Time if required.
6. Click Apply.

Figure 147: Configuring a Voice VLAN

Traffic > VoIP

Step: 1. Configure Global

Auto Detection Status ☒ Enabled

Voice VLAN 1234

Voice VLAN Aging Time (5-43200) 3000 sec

Apply Revert

CONFIGURING TELEPHONY OUI

VoIP devices attached to the switch can be identified by the vendor's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to vendors 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. Use the Traffic > VoIP (Configure OUI) page to configure this feature.

CLI REFERENCES

- ◆ ["Configuring Voice VLANs" on page 1160](#)

PARAMETERS

These parameters are displayed:

- ◆ **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- ◆ **Mask** – Identifies a range of MAC addresses. 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 FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- ◆ **Description** – User-defined text that identifies the VoIP devices.

WEB INTERFACE

To configure MAC OUI numbers for VoIP equipment:

1. Click Traffic, VoIP.
2. Select Configure OUI from the Step list.
3. Select Add from the Action list.
4. Enter a MAC address that specifies the OUI for VoIP devices in the network.

5. Select a mask from the pull-down list to define a MAC address range.
6. Enter a description for the devices.
7. Click Apply.

Figure 148: Configuring an OUI Telephony List

Traffic > VoIP

Step: 2. Configure OUI Action: Add

Telephony OUI: 00-e0-bb-00-00-00

Mask: FF-FF-FF-00-00-00

Description: old phones

Apply Revert

To show the MAC OUI numbers used for VoIP equipment:

1. Click Traffic, VoIP.
2. Select Configure OUI from the Step list.
3. Select Show from the Action list.

Figure 149: Showing an OUI Telephony List

Traffic > VoIP

Step: 2. Configure OUI Action: Show

Telephony OUI List Total: 3

<input type="checkbox"/>	Telephony OUI	Mask	Description
<input type="checkbox"/>	00-E0-BB-00-00-00	FF-FF-FF-00-00-00	old phones
<input type="checkbox"/>	00-11-22-33-44-55	FF-FF-FF-00-00-00	new phones
<input type="checkbox"/>	00-98-76-54-32-10	FF-FF-FF-FF-FF-FF	Chris' phone

Delete Revert

CONFIGURING VOIP TRAFFIC PORTS

Use the Traffic > VoIP (Configure Interface) page to configure ports for VoIP traffic, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only VoIP traffic is forwarded on the Voice VLAN.

CLI REFERENCES

- ◆ ["Configuring Voice VLANs" on page 1160](#)

COMMAND USAGE

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), first ensure that VLAN membership is not set to access mode (see ["Adding Static Members to VLANs" on page 199](#)).

PARAMETERS

These parameters are displayed:

- ◆ **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)
 - **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be 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. You must select a method for detecting VoIP traffic, either OUI or 802.1ab (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.
 - **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
- ◆ **Security** – Enables security filtering that 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. (Default: Disabled)
- ◆ **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
 - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to vendors and form the first three octets of a device MAC address. 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** – Uses LLDP (IEEE 802.1AB) to discover VoIP devices attached to the port. LLDP checks that the "telephone bit" in the system capability TLV is turned on. See ["Link Layer Discovery Protocol" on page 416](#) for more information on LLDP.
- ◆ **Priority** – Defines a CoS priority for port 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. (Range: 0-6; Default: 6)
- ◆ **Remaining Age** – Number of minutes before this entry is aged out. The Remaining Age starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging

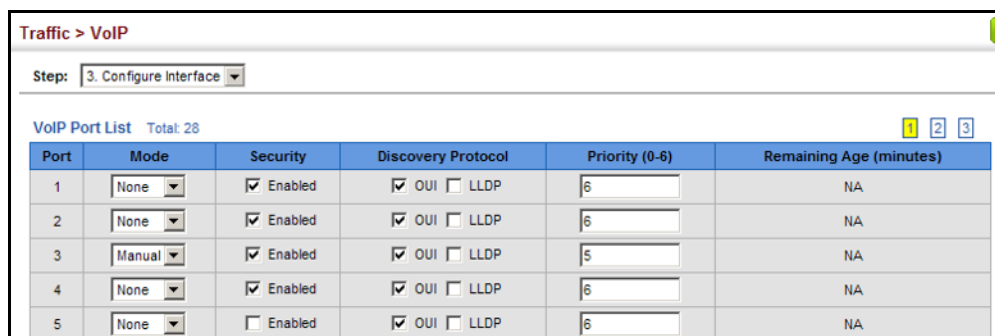
time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the Remaining Age.

WEB INTERFACE

To configure VoIP traffic settings for a port:

1. Click Traffic, VoIP.
2. Select Configure Interface from the Step list.
3. Configure any required changes to the VoIP settings each port.
4. Click Apply.

Figure 150: Configuring Port Settings for a Voice VLAN



Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
2	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
3	Manual	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	5	NA
4	None	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
5	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA

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 to the data ports. This switch provides secure network management access using the following options:

- ◆ [AAA](#) – Use local or remote authentication to configure access rights, specify authentication servers, configure remote authentication and accounting.
- ◆ [User Accounts](#) – Manually configure access rights on the switch for specified users.
- ◆ [Web Authentication](#) – Allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication methods are infeasible or impractical.
- ◆ [Network Access](#) – Configure MAC authentication, intrusion response, dynamic VLAN assignment, and dynamic QoS assignment.
- ◆ [HTTPS](#) – Provide a secure web connection.
- ◆ [SSH](#) – Provide a secure shell (for secure Telnet access).
- ◆ [ACL](#) – Access Control Lists provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code).
- ◆ [ARP Inspection](#) – Security feature that validates the MAC Address bindings for Address Resolution Protocol packets. Provides protection against ARP traffic with invalid MAC to IP Address bindings, which forms the basis for certain “man-in-the-middle” attacks.
- ◆ [IP Filter](#) – Filters management access to the web, SNMP or Telnet interface.
- ◆ [Port Security](#) – Configure secure addresses for individual ports.
- ◆ [Port Authentication](#) – Use IEEE 802.1X port authentication to control access to specific ports.
- ◆ [DoS Protection](#) – Protects against Denial-of-Service attacks.
- ◆ [IP Source Guard](#) – Filters untrusted DHCP messages on insecure ports by building and maintaining a DHCP snooping binding table.

- ◆ **DHCP Snooping** – Filter IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping.



NOTE: The priority of execution for the filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, IP Source Guard, and then DHCP Snooping.

AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING)

The authentication, authorization, and accounting (AAA) feature provides the main framework for configuring access control on the switch. The three security functions can be summarized as follows:

- ◆ **Authentication** — Identifies users that request access to the network.
- ◆ **Authorization** — Determines if users can access specific services.
- ◆ **Accounting** — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The switch supports the following AAA features:

- ◆ Accounting for IEEE 802.1X authenticated users that access the network through the switch.
- ◆ Accounting for users that access management interfaces on the switch through the console and Telnet.
- ◆ Accounting for commands that users enter at specific CLI privilege levels.
- ◆ Authorization of users that access management interfaces on the switch through the console and Telnet.

To configure AAA on the switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See ["Configuring Local/Remote Logon Authentication" on page 307](#).
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.

3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use.
4. Apply the method names to port or line interfaces.



NOTE: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS or TACACS+ server software.

CONFIGURING LOCAL/ REMOTE LOGON AUTHENTICATION

Use the Security > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

CLI REFERENCES

- ◆ ["Authentication Sequence" on page 827](#)

COMMAND USAGE

- ◆ By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence. Then specify the corresponding parameters for the remote authentication protocol using the Security > AAA > Server page. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- ◆ You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

PARAMETERS

These parameters are displayed:

- ◆ **Authentication Sequence** – Select the authentication, or authentication sequence required:
 - **Local** – User authentication is performed only locally by the switch.
 - **RADIUS** – User authentication is performed using a RADIUS server only.
 - **TACACS** – User authentication is performed using a TACACS+ server only.

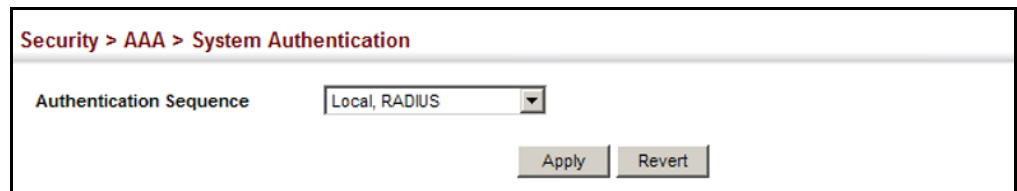
- [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

WEB INTERFACE

To configure the method(s) of controlling management access:

1. Click Security, AAA, System Authentication.
2. Specify the authentication sequence (i.e., one to three methods).
3. Click Apply.

Figure 151: Configuring the Authentication Sequence

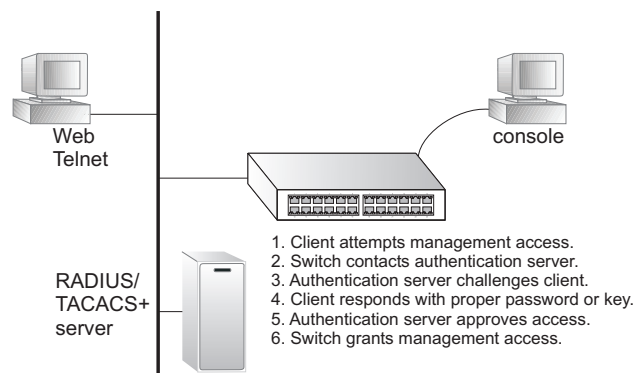


CONFIGURING REMOTE LOGON AUTHENTICATION SERVERS

Use the Security > AAA > Server page to configure the message exchange parameters for RADIUS or TACACS+ remote access authentication servers.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or 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 that requires management access to the switch.

Figure 152: Authentication Server Operation



RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a more reliable 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.

CLI REFERENCES

- ◆ "RADIUS Client" on page 830
- ◆ "TACACS+ Client" on page 834
- ◆ "AAA" on page 838

COMMAND USAGE

- ◆ If a remote authentication server is used, you must specify the message exchange parameters for the remote authentication protocol. Both local and remote logon authentication control management access via the console port, web browser, or Telnet.
- ◆ RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

PARAMETERS

These parameters are displayed:

Configure Server

◆ RADIUS

- **Global** – Provides globally applicable RADIUS settings.
- **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
- **Server IP Address** – Address of authentication server.
(A Server Index entry must be selected to display this item.)
- **Accounting Server UDP Port** – Network (UDP) port on authentication server used for accounting messages.
(Range: 1-65535; Default: 1813)
- **Authentication Server UDP Port** – Network (UDP) port on authentication server used for authentication messages.
(Range: 1-65535; Default: 1812)
- **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
- **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server.
(Range: 1-30; Default: 2)

- **Set Key** – Mark this box to set or modify the encryption key.
- **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

◆ **TACACS+**

- **Global** – Provides globally applicable TACACS+ settings.
- **Server Index** – Specifies the index number of the server to be configured. The switch currently supports only one TACACS+ server.
- **Server IP Address** – Address of the TACACS+ server.
(A Server Index entry must be selected to display this item.)
- **Authentication Server TCP Port** – Network (TCP) port of TACACS+ server used for authentication messages.
(Range: 1-65535; Default: 49)
- **Authentication Timeout** – The number of seconds the switch waits for a reply from the TACACS+ server before it resends the request. (Range: 1-65535; Default: 5)
- **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server.
(Range: 1-30; Default: 2)
- **Set Key** – Mark this box to set or modify the encryption key.
- **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

Configure Group

- ◆ **Server Type** – Select RADIUS or TACACS+ server.
- ◆ **Group Name** – Defines a name for the RADIUS or TACACS+ server group. (Range: 1-64 characters)
- ◆ **Sequence at Priority** – Specifies the server and sequence to use for the group. (Range: 1-5 for RADIUS; 1 for TACACS)

When specifying the priority sequence for a sever, the server index must already be defined (see ["Configuring Local/Remote Logon Authentication" on page 307](#)).

WEB INTERFACE

To configure the parameters for RADIUS or TACACS+ authentication:

1. Click Security, AAA, Server.
2. Select Configure Server from the Step list.
3. Select RADIUS or TACACS+ server type.
4. Select Global to specify the parameters that apply globally to all specified servers, or select a specific Server Index to specify the parameters that apply to a specific server.
5. To set or modify the authentication key, mark the Set Key box, enter the key, and then confirm it
6. Click Apply.

Figure 153: Configuring Remote Authentication Server (RADIUS)

The screenshot displays the 'Security > AAA > Server' configuration page. At the top, 'Server Type' is set to 'RADIUS' and 'Server Index' is set to '1'. The 'Global' radio button is selected. The following fields are configured: 'Server IP Address' is 10.1.1.1, 'Accounting Server UDP Port (1-65535)' is 1813, 'Authentication Server UDP Port (1-65535)' is 1815, 'Authentication Timeout (1-65535)' is 10 seconds, and 'Authentication Retries (1-30)' is 5. The 'Set Key' checkbox is checked. The 'Authentication Key' and 'Confirm Authentication Key' fields are masked with dots. 'Apply' and 'Revert' buttons are located at the bottom right.

Figure 154: Configuring Remote Authentication Server (TACACS+)

Security > AAA > Server

Step: 1. Configure Server

Server Type ☐ RADIUS ☒ TACACS+

☐ Global | Server Index: ☒ 1

Server IP Address

Authentication Server TCP Port (1-65535)

Authentication Timeout (1-540) sec

Authentication Retries (1-30)

☒ Set Key

Authentication Key

Confirm Authentication Key

Apply Revert

To configure the RADIUS or TACACS+ server groups to use for accounting and authorization:

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Select RADIUS or TACACS+ server type.
5. Enter the group name, followed by the index of the server to use for each priority level.
6. Click Apply.

Figure 155: Configuring AAA Server Groups

Security > AAA > Server

Step: 2. Configure Group Action: Add

Server Type ☒ RADIUS ☐ TACACS+

RADIUS Group Name

Sequence At Priority 1

Sequence At Priority 2

Sequence At Priority 3

Sequence At Priority 4

Sequence At Priority 5

Apply Revert

To show the RADIUS or TACACS+ server groups used for accounting and authorization:

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 156: Showing AAA Server Groups

The screenshot shows the 'Security > AAA > Server' configuration page. At the top, there is a breadcrumb trail. Below it, a 'Step' dropdown is set to '2. Configure Group' and an 'Action' dropdown is set to 'Show'. Under 'Server Type', the 'RADIUS' radio button is selected. The 'RADIUS Group List' section shows a table with 3 groups. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Group Name	Member Index
<input type="checkbox"/>	radius	1, 2, 3, 5
<input type="checkbox"/>	radius1	3, 5, 1
<input type="checkbox"/>	radius2	1, 2, 5

CONFIGURING AAA ACCOUNTING

Use the Security > AAA > Accounting page to enable accounting of requested services for billing or security purposes, and also to display the configured accounting methods, the methods applied to specific interfaces, and basic accounting information recorded for user sessions.

CLI REFERENCES

- ◆ ["AAA" on page 838](#)

COMMAND USAGE

AAA authentication through a RADIUS or TACACS+ server must be enabled before accounting is enabled.

PARAMETERS

These parameters are displayed:

Configure Global

- ◆ **Periodic Update** - Specifies the interval at which the local accounting service updates information for all users on the system to the accounting server. (Range: 1-2147483647 minutes)

Configure Method

- ◆ **Accounting Type** – Specifies the service as:
 - **802.1X** – Accounting for end users.
 - **Command** – Administrative accounting to apply to commands entered at specific CLI privilege levels.

- **Exec** – Administrative accounting for local console, Telnet, or SSH connections.
- ◆ **Privilege Level** – The CLI privilege levels (0-15). This parameter only applies to Command accounting.
- ◆ **Method Name** – Specifies an accounting method for service requests. The “default” methods are used for a requested service if no other methods have been defined. (Range: 1-64 characters)

Note that the method name is only used to describe the accounting method configured on the specified RADIUS or TACACS+ servers. No information is sent to the servers about the method to use.
- ◆ **Accounting Notice** – Records user activity from log-in to log-off point.
- ◆ **Server Group Name** - Specifies the accounting server group. (Range: 1-64 characters)

The group names “radius” and “tacacs+” specifies all configured RADIUS and TACACS+ hosts (see ["Configuring Local/Remote Logon Authentication" on page 307](#)). Any other group name refers to a server group configured on the Security > AAA > Server (Configure Group) page.

Configure Service

- ◆ **Accounting Type** – Specifies the service as 802.1X, Command or Exec as described in the preceding section.
- ◆ **802.1X**
 - **Method Name** – Specifies a user defined accounting method to apply to an interface. This method must be defined in the Configure Method page. (Range: 1-64 characters)
- ◆ **Command**
 - **Privilege Level** – The CLI privilege levels (0-15).
 - **Console Method Name** – Specifies a user-defined method name to apply to commands entered at the specified CLI privilege level through the console interface.
 - **VTY Method Name** – Specifies a user-defined method name to apply to commands entered at the specified CLI privilege level through Telnet.
- ◆ **Exec**
 - **Console Method Name** – Specifies a user defined method name to apply to console connections.
 - **VTY Method Name** – Specifies a user defined method name to apply to Telnet connections.

Show Information – Summary

- ◆ **Accounting Type** - Displays the accounting service.
- ◆ **Method Name** - Displays the user-defined or default accounting method.
- ◆ **Server Group Name** - Displays the accounting server group.
- ◆ **Interface** - Displays the port, console or Telnet interface to which these rules apply. (This field is null if the accounting method and associated server group has not been assigned to an interface.)

Show Information – Statistics

- ◆ **User Name** - Displays a registered user name.
- ◆ **Accounting Type** - Displays the accounting service.
- ◆ **Interface** - Displays the receive port number through which this user accessed the switch.
- ◆ **Time Elapsed** - Displays the length of time this entry has been active.

WEB INTERFACE

To configure global settings for AAA accounting:

1. Click Security, AAA, Accounting.
2. Select Configure Global from the Step list.
3. Enter the required update interval.
4. Click Apply.

Figure 157: Configuring Global Settings for AAA Accounting

Security > AAA > Accounting

Step: 1. Configure Global

Periodic Update (1-2147483647) ☒ 1 min

Apply Revert

To configure the accounting method applied to various service types and the assigned server group:

1. Click Security, AAA, Accounting.
2. Select Configure Method from the Step list.
3. Select Add from the Action list.

4. Select the accounting type (802.1X, Command, Exec).
5. Specify the name of the accounting method and server group name.
6. Click Apply.

Figure 158: Configuring AAA Accounting Methods

Security > AAA > Accounting

Step: 2. Configure Method Action: Add

Accounting Type: 802.1X

Method Name: default

Accounting Notice: Start-Stop

Server Group Name: ☒ radius ☐

Apply Revert

To show the accounting method applied to various service types and the assigned server group:

1. Click Security, AAA, Accounting.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

Figure 159: Showing AAA Accounting Methods

Security > AAA > Accounting

Step: 2. Configure Method Action: Show

Method List Total: 18

<input type="checkbox"/>	Accounting Type	Method Name	Accounting Notice	Server Group Name
<input type="checkbox"/>	802.1X	default	Start-Stop	radius
<input type="checkbox"/>	Command 0	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 1	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 2	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 3	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 4	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 5	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 6	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 7	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 8	default	Start-Stop	tacacs+

Delete Revert

To configure the accounting method applied to specific interfaces, console commands entered at specific privilege levels, and local console, Telnet, or SSH connections:

1. Click Security, AAA, Accounting.
2. Select Configure Service from the Step list.
3. Select the accounting type (802.1X, Command, Exec).
4. Enter the required accounting method.
5. Click Apply.

Figure 160: Configuring AAA Accounting Service for 802.1X Service

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type: ☒ 802.1X ☐ Command ☐ EXEC

Port Method List Total: 26

Port	Method Name
1	default
2	default
3	default
4	
5	

Figure 161: Configuring AAA Accounting Service for Command Service

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type: ☐ 802.1X ☒ Command ☐ EXEC

Command Method List Total: 16

Privilege Level	Console Method Name	VTY Method Name
0	default	default
1	default	default
2	default	default
3	default	default
4	command4Method	default
5	default	command5Method

Figure 162: Configuring AAA Accounting Service for Exec Service

The screenshot shows the 'Security > AAA > Accounting' configuration page. The 'Step' dropdown is set to '3. Configure Service'. Under 'Accounting Type', the 'EXEC' radio button is selected. The 'Console Method Name' and 'VTY Method Name' text boxes both contain the value 'default'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To display a summary of the configured accounting methods and assigned server groups for specified service types:

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Summary.

Figure 163: Displaying a Summary of Applied AAA Accounting Methods

The screenshot shows the 'Security > AAA > Accounting' configuration page with the 'Step' dropdown set to '4. Show Information'. The 'Summary' radio button is selected. Below the tabs, it says 'Method List Total: 18'. A table displays the applied accounting methods.

Accounting Type	Method Name	Server Group Name	Interface
802.1X	default	radius	
Command 0	default	tacacs+	
Command 1	default	tacacs+	
Command 2	default	tacacs+	
Command 3	default	tacacs+	
Command 4	default	tacacs+	
Command 5	default	tacacs+	
Command 6	default	tacacs+	
Command 7	default	tacacs+	
Command 8	default	tacacs+	

To display basic accounting information and statistics recorded for user sessions:

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Statistics.

Figure 164: Displaying Statistics for AAA Accounting Sessions

Security > AAA > Accounting			
Step: 4. Show Information			
<input type="radio"/> Summary <input checked="" type="radio"/> Statistics			
Accounting Statistics Total: 2			
User Name	Accounting Type	Interface	Time Elapsed
Bob	802.1X	Eth1/1	3:44:55
Ted	802.1X	Eth1/5	1:24:51

CONFIGURING AAA AUTHORIZATION

Use the Security > AAA > Authorization page to enable authorization of requested services, and also to display the configured authorization methods, and the methods applied to specific interfaces.

CLI REFERENCES

- ◆ ["AAA" on page 838](#)

COMMAND USAGE

- ◆ This feature performs authorization to determine if a user is allowed to run an Exec shell.
- ◆ AAA authentication through a RADIUS or TACACS+ server must be enabled before authorization is enabled.

PARAMETERS

These parameters are displayed:

Configure Method

- ◆ **Authorization Type** – Specifies the service as Exec, indicating administrative authorization for local console, Telnet, or SSH connections.
- ◆ **Method Name** – Specifies an authorization method for service requests. The "default" method is used for a requested service if no other methods have been defined. (Range: 1-64 characters)
- ◆ **Server Group Name** - Specifies the authorization server group. (Range: 1-64 characters)

The group name "tacacs+" specifies all configured TACACS+ hosts (see ["Configuring Local/Remote Logon Authentication" on page 307](#)). Any other group name refers to a server group configured on the TACACS+ Group Settings page. Authorization is only supported for TACACS+ servers.

Configure Service

- ◆ **Authorization Type** – Specifies the service as Exec, indicating administrative authorization for local console, Telnet, or SSH connections.

- ◆ **Console Method Name** – Specifies a user defined method name to apply to console connections.
- ◆ **VTY Method Name** – Specifies a user defined method name to apply to Telnet connections.

Show Information

- ◆ **Authorization Type** - Displays the authorization service.
- ◆ **Method Name** - Displays the user-defined or default accounting method.
- ◆ **Server Group Name** - Displays the authorization server group.
- ◆ **Interface** - Displays the console or Telnet interface to which these rules apply. (This field is null if the authorization method and associated server group has not been assigned to an interface.)

WEB INTERFACE

To configure the authorization method applied to the Exec service type and the assigned server group:

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Specify the name of the authorization method and server group name.
4. Click Apply.

Figure 165: Configuring AAA Authorization Methods

The screenshot shows a web interface for configuring AAA Authorization. The breadcrumb path is "Security > AAA > Authorization". Below this, there are two dropdown menus: "Step:" set to "1. Configure Method" and "Action:" set to "Add". The main configuration area has three fields: "Authorization Type" with a dropdown menu showing "EXEC", "Method Name" with a text input field containing "default", and "Server Group Name" with a radio button selection. The "tacacs+" option is selected, and there is an empty text input field next to it. At the bottom right, there are two buttons: "Apply" and "Revert".

To show the authorization method applied to the EXEC service type and the assigned server group:

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

Figure 166: Showing AAA Authorization Methods

Security > AAA > Authorization

Step: 1. Configure Method Action: Show

Method List Total: 2

	Authorization Type	Method Name	Server Group Name
<input type="checkbox"/>	EXEC	default	tacacs+
<input type="checkbox"/>	EXEC	aaa	tacacs1

Delete Revert

To configure the authorization method applied to local console, Telnet, or SSH connections:

1. Click Security, AAA, Authorization.
2. Select Configure Service from the Step list.
3. Enter the required authorization method.
4. Click Apply.

Figure 167: Configuring AAA Authorization Methods for Exec Service

Security > AAA > Authorization

Step: 2. Configure Service

Authorization Type EXEC

Console Method Name tps-auth

VTY Method Name tps-auth

Apply Revert

To display a the configured authorization method and assigned server groups for The Exec service type:

1. Click Security, AAA, Authorization.
2. Select Show Information from the Step list.

Figure 168: Displaying the Applied AAA Authorization Method

Security > AAA > Authorization

Step: 3. Show Information

Method List Total: 3

Authorization Type	Method Name	Server Group Name	Interface
EXEC	default	tacacs+	
EXEC	console	tacacs+	Console
EXEC	telnet	tacacs+	Telnet

CONFIGURING USER ACCOUNTS

Use the Security > User Accounts page to control management access to the switch based on manually configured user names and passwords.

CLI REFERENCES

- ◆ ["User Accounts and Privilege Levels" on page 824](#)

COMMAND USAGE

- ◆ The default guest name is "guest" with the password "guest." The default administrator name is "admin" with the password "admin."
- ◆ The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

PARAMETERS

These parameters are displayed:

- ◆ **User Name** – The name of the user.
(Maximum length: 32 characters; maximum number of users: 16)
- ◆ **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged)

Normal privilege level 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. Privileged level provides full access to all commands.
- ◆ **Password Type** – Specifies the following options:
 - **No Password** – No password is required for this user to log in.
 - **Plain Password** – Plain text unencrypted password.
 - **Encrypted Password** – Encrypted password.

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 or when downloading the configuration file from a TFTP or FTP server. There is no need for you to manually configure encrypted passwords.
- ◆ **Password** – Specifies the user password.
(Range: 0-32 characters, case sensitive)
- ◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

WEB INTERFACE

To configure user accounts:

1. Click Security, User Accounts.
2. Select Add from the Action list.
3. Specify a user name, select the user's access level, then enter a password if required and confirm it.
4. Click Apply.

Figure 169: Configuring User Accounts

Security > User Accounts

Action: Add

User Name:

Access Level: 15 (Privileged)

Password Type: Plain Password

Password:

Confirm Password:

Apply Revert

To show user accounts:

1. Click Security, User Accounts.
2. Select Show from the Action list.

Figure 170: Showing User Accounts

Security > User Accounts

Action: Show

User Account List Total: 3

<input type="checkbox"/>	User Name	Access Level
<input type="checkbox"/>	admin	15
<input type="checkbox"/>	guest	0
<input type="checkbox"/>	bob	15

Delete Revert

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 properly for the web authentication feature to work properly. (See ["Configuring Local/Remote Logon Authentication" on page 307.](#))

NOTE: Web authentication cannot be configured on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication (Configure Global) page to edit the global parameters for web authentication.

CLI REFERENCES

- ◆ ["Web Authentication" on page 905](#)

PARAMETERS

These parameters are displayed:

- ◆ **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled)

Note that this feature must also be enabled for any port where required under the Configure Interface menu.
- ◆ **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600 seconds)
- ◆ **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)
- ◆ **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

WEB INTERFACE

To configure global parameters for web authentication:

1. Click Security, Web Authentication.
2. Select Configure Global from the Step list.
3. Enable web authentication globally on the switch, and adjust any of the protocol parameters as required.
4. Click Apply.

Figure 171: Configuring Global Settings for Web Authentication

Security > Web Authentication

Step: 1. Configure Global

Web Authentication Status ☐ Enabled

Session Timeout (300-3600) 3600 sec

Quiet Period (1-180) 60 sec

Login Attempts (1-3) 3

Apply Revert

CONFIGURING INTERFACE SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication (Configure Interface) page to enable web authentication on a port, and display information for any connected hosts.

CLI REFERENCES

- ◆ ["Web Authentication" on page 905](#)

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Indicates the port being configured.
- ◆ **Status** – Configures the web authentication status for the port.
- ◆ **Host IP Address** – Indicates the IP address of each connected host.
- ◆ **Remaining Session Time** – Indicates the remaining time until the current authorization session for the host expires.
- ◆ **Apply** – Enables web authentication if the Status box is checked.
- ◆ **Revert** – Restores the previous configuration settings.
- ◆ **Re-authenticate** – Ends all authenticated web sessions for selected host IP addresses in the Authenticated Host List, and forces the users to re-authenticate.

WEB INTERFACE

To enable web authentication for a port:

1. Click Security, Web Authentication.
2. Select Configure Interface from the Step list.
3. Set the status box to enabled for any port that requires web authentication, and click Apply
4. Mark the check box for any host addresses that need to be re-authenticated, and click Re-authenticate.

Figure 172: Configuring Interface Settings for Web Authentication

Security > Web Authentication

Step: 2. Configure Interface

Port: 1

Status: ☒ Enabled

Apply Revert

Authenticated Host List Total: 2

<input type="checkbox"/>	Host IP Address	Remaining Session Time (sec)
<input type="checkbox"/>	10.1.1.1	300
<input type="checkbox"/>	10.2.2.2	100

Re-authenticate Revert

NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

Some devices connected to switch ports may not be able to support 802.1X authentication due to hardware or software limitations. This is often true for devices such as network printers, IP phones, and some wireless access points. The switch enables network access from these devices to be controlled by authenticating device MAC addresses with a central RADIUS server.



NOTE: RADIUS authentication must be activated and configured properly for the MAC Address authentication feature to work properly. (See ["Configuring Remote Logon Authentication Servers" on page 308.](#))

NOTE: MAC authentication cannot be configured on trunk ports.

CLI REFERENCES

- ◆ ["Network Access \(MAC Address Authentication\)" on page 892](#)

COMMAND USAGE

- ◆ MAC address 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. On successful authentication, the RADIUS server may optionally assign VLAN and quality of service settings for the switch port.

- ◆ 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.
- ◆ When port status changes to down, all MAC addresses mapped to that port are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- ◆ The RADIUS server may optionally return a VLAN identifier list to be applied to the switch port. The following attributes need to be configured on the RADIUS server.
 - **Tunnel-Type** = VLAN
 - **Tunnel-Medium-Type** = 802
 - **Tunnel-Private-Group-ID** = 1u,2t [VLAN ID list]

The VLAN identifier list is carried in the RADIUS "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t,3u" where "u" indicates an untagged VLAN and "t" a tagged VLAN.

- ◆ 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 19: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	service-policy-in = <i>policy-map-name</i>	service-policy-in=p1
Rate Limit	rate-limit-input = <i>rate</i>	rate-limit-input=100 (in units of Kbps)
802.1p	switchport-priority-default = <i>value</i>	switchport-priority-default=2

Table 19: Dynamic QoS Profiles (Continued)

Profile	Attribute Syntax	Example
IP ACL	ip-access-group-in = <i>ip-acl-name</i>	ip-access-group-in=ip4acl
IPv6 ACL	ipv6-access-group-in = <i>ipv6-acl-name</i>	ipv6-access-group-in=ipv6acl
MAC ACL	mac-access-group-in = <i>mac-acl-name</i>	mac-access-group-in=macAcl

- ◆ Multiple profiles can be specified in the Filter-ID attribute by using a semicolon to separate each profile.
For example, the attribute "service-policy-in=pp1;rate-limit-input=100" specifies that the diffserv profile name is "pp1," and the ingress rate limit profile value is 100 kbps.
- ◆ If duplicate profiles are passed in the Filter-ID attribute, then only the first profile is used.
For example, if the attribute is "service-policy-in=p1;service-policy-in=p2", then the switch applies only the DiffServ profile "p1."
- ◆ Any unsupported profiles in the Filter-ID attribute are ignored.
For example, if the attribute is "map-ip-dscp=2:3;service-policy-in=p1," then the switch ignores the "map-ip-dscp" profile.
- ◆ When authentication is successful, the dynamic QoS information may not be passed from the RADIUS server due to one of the following conditions (authentication result remains unchanged):
 - The Filter-ID attribute cannot be found to carry the user profile.
 - The Filter-ID attribute is empty.
 - The Filter-ID attribute format for dynamic QoS assignment is unrecognizable (can not recognize the whole Filter-ID attribute).
- ◆ Dynamic QoS assignment fails and the authentication result changes from success to failure when the following conditions occur:
 - Illegal characters found in a profile value (for example, a non-digital character in an 802.1p profile value).
 - Failure to configure the received profiles on the authenticated port.
- ◆ When the last user logs off on 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 the port.

CONFIGURING GLOBAL SETTINGS FOR NETWORK ACCESS

MAC address authentication is configured on a per-port basis, however there are two configurable parameters that apply globally to all ports on the switch. Use the Security > Network Access (Configure Global) page to configure MAC address authentication aging and reauthentication time.

CLI REFERENCES

- ◆ ["Network Access \(MAC Address Authentication\)" on page 892](#)

PARAMETERS

These parameters are displayed:

- ◆ **Aging Status** – Enables aging for authenticated MAC addresses stored in the secure MAC address table. (Default: Disabled)

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 385](#)).

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 maximum number of secure MAC addresses supported for the switch system is 1024.

- ◆ **Reauthentication Time** – Sets the time period after which a connected host must be reauthenticated. 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. (Range: 120-1000000 seconds; Default: 1800 seconds)

WEB INTERFACE

To configure aging status and reauthentication time for MAC address authentication:

1. Click Security, Network Access.
2. Select Configure Global from the Step list.
3. Enable or disable aging for secure addresses, and modify the reauthentication time as required.
4. Click Apply.

Figure 173: Configuring Global Settings for Network Access

Security > Network Access

Step: 1. Configure Global

Aging Status ☒ Enabled

Reauthentication Time (120-1000000) 30000 sec

Apply Revert

CONFIGURING NETWORK ACCESS FOR PORTS

Use the Security > Network Access (Configure Interface - General) page to configure MAC authentication on switch ports, including enabling address authentication, setting the maximum MAC count, and enabling dynamic VLAN or dynamic QoS assignments.

CLI REFERENCES

- ◆ ["Network Access \(MAC Address Authentication\)" on page 892](#)

PARAMETERS

These parameters are displayed:

◆ MAC Authentication

- **Status** – Enables MAC authentication on a port. (Default: Disabled)
- **Intrusion** – Sets the port response to a host MAC authentication failure to either block access to the port or to pass traffic through. (Options: Block, Pass; Default: Block)
- **Max MAC Count**¹¹ – Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication; that is, the Network Access process described in this section. (Range: 1-1024; Default: 1024)
- ◆ **Network Access Max MAC Count**¹¹ – Sets the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication (including Network Access and IEEE 802.1X). (Range: 1-2048; Default: 1024)
- ◆ **Guest VLAN** – Specifies the VLAN to be assigned to the port when 802.1X Authentication fails. (Range: 0-4093, where 0 means disabled; Default: Disabled)

The VLAN must already be created and active (see ["Configuring VLAN Groups" on page 196](#)). Also, when used with 802.1X authentication, intrusion action must be set for "Guest VLAN" (see ["Configuring Port Authenticator Settings for 802.1X" on page 385](#)).

11. 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.

- ◆ **Dynamic VLAN** – Enables dynamic VLAN assignment for an authenticated port. When enabled, any VLAN identifiers returned by the RADIUS server through the 802.1X authentication process are applied to the port, providing the VLANs have already been created on the switch. (GVRP is not used to create the VLANs.) (Default: Enabled)

The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have the same VLAN configuration, or they are treated as authentication failures.

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 is assigned to the default untagged VLAN.

When the dynamic VLAN assignment status is changed on a port, all authenticated addresses mapped to that port are cleared from the secure MAC address table.

- ◆ **Dynamic QoS** – Enables dynamic QoS assignment for an authenticated port. (Default: Disabled)
- ◆ **MAC Filter ID** – Allows a MAC Filter to be assigned to the port. MAC addresses or MAC address ranges present in a selected MAC Filter are exempt from authentication on the specified port (as described under ["Configuring a MAC Address Filter"](#)). (Range: 1-64; Default: None)

WEB INTERFACE

To configure MAC authentication on switch ports:

1. Click Security, Network Access.
2. Select Configure Interface from the Step list.
3. Click the General button.
4. Make any configuration changes required to enable address authentication on a port, set the maximum number of secure addresses supported, the guest VLAN to use when MAC Authentication or 802.1X Authentication fails, and the dynamic VLAN and QoS assignments.
5. Click Apply.

Figure 174: Configuring Interface Settings for Network Access

Security > Network Access

Step: 2. Configure Interface

General Link Detection

Port List Total: 28

Port	MAC Authentication			Network Access Max MAC Count (1-2048)	Guest VLAN (0-4093, 0: Disabled)	Dynamic VLAN	Dynamic QoS	MAC Filter ID (1-64)
	Status	Intrusion	Max MAC Count (1-1024)					
1	<input type="checkbox"/> Enabled	Block	1024	1024	0	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> 1
2	<input checked="" type="checkbox"/> Enabled	Block	1024	1024	0	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> 1
3	<input type="checkbox"/> Enabled	Block	1024	1024	0	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> 1
4	<input type="checkbox"/> Enabled	Block	1024	1024	0	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> 1
5	<input type="checkbox"/> Enabled	Block	1024	1024	0	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> 1

CONFIGURING PORT LINK DETECTION Use the Security > Network Access (Configure Interface - Link Detection) page to send an SNMP trap and/or shut down a port when a link event occurs.

CLI REFERENCES

- ◆ ["Network Access \(MAC Address Authentication\)" on page 892](#)

PARAMETERS

These parameters are displayed:

- ◆ **Link Detection Status** – Configures whether Link Detection is enabled or disabled for a port.
- ◆ **Condition** – The link event type which will trigger the port action.
 - **Link up** – Only link up events will trigger the port action.
 - **Link down** – Only link down events will trigger the port action.
 - **Link up and down** – All link up and link down events will trigger the port action.
- ◆ **Action** – The switch can respond in three ways to a link up or down trigger event.
 - **Trap** – An SNMP trap is sent.
 - **Trap and shutdown** – An SNMP trap is sent and the port is shut down.
 - **Shutdown** – The port is shut down.

WEB INTERFACE

To configure link detection on switch ports:

1. Click Security, Network Access.
2. Select Configure Interface from the Step list.
3. Click the Link Detection button.
4. Modify the link detection status, trigger condition, and the response for any port.
5. Click Apply.

Figure 175: Configuring Link Detection for Network Access

Security > Network Access

Step: 2. Configure Interface

General Link Detection

Port List Total: 28

Port	Link Detection Status	Condition	Action
1	<input type="checkbox"/> Enabled	Link down	Trap
2	<input checked="" type="checkbox"/> Enabled	Link up and down	Trap
3	<input type="checkbox"/> Enabled	Link down	Trap
4	<input type="checkbox"/> Enabled	Link down	Trap
5	<input type="checkbox"/> Enabled	Link down	Trap

CONFIGURING A MAC ADDRESS FILTER

Use the Security > Network Access (Configure MAC Filter) page to designate specific MAC addresses or MAC address ranges as exempt from authentication. MAC addresses present in MAC Filter tables activated on a port are treated as pre-authenticated on that port.

CLI REFERENCES

- ◆ ["Network Access \(MAC Address Authentication\)" on page 892](#)

COMMAND USAGE

- ◆ Specified MAC addresses are exempt from authentication.
- ◆ Up to 65 filter tables can be defined.
- ◆ There is no limitation on the number of entries used in a filter table.

PARAMETERS

These parameters are displayed:

- ◆ **Filter ID** – Adds a filter rule for the specified filter.
- ◆ **MAC Address** – The filter rule will check ingress packets against the entered MAC address or range of MAC addresses (as defined by the MAC Address Mask).

- ◆ **MAC Address Mask** – The filter rule will check for the range of MAC addresses defined by the MAC bit mask. If you omit the mask, the system will assign the default mask of an exact match.
(Range: 000000000000 - FFFFFFFF; Default: FFFFFFFF)

WEB INTERFACE

To add a MAC address filter for MAC authentication:

1. Click Security, Network Access.
2. Select Configure MAC Filter from the Step list.
3. Select Add from the Action list.
4. Enter a filter ID, MAC address, and optional mask.
5. Click Apply.

Figure 176: Configuring a MAC Address Filter for Network Access

Security > Network Access

Step: 3. Configure MAC Filter Action: Add

Filter ID (1-64) 22

MAC Address 11-22-33-44-55-66

MAC Address Mask FFFFFFFFFF

Apply Revert

To show the MAC address filter table for MAC authentication:

1. Click Security, Network Access.
2. Select Configure MAC Filter from the Step list.
3. Select Show from the Action list.

Figure 177: Showing the MAC Address Filter Table for Network Access

Security > Network Access

Step: 3. Configure MAC Filter Action: Show

MAC Filter List Total: 1

<input type="checkbox"/>	Filter ID	MAC Address	MAC Address Mask
<input checked="" type="checkbox"/>	22	11-22-33-44-55-66	FF-FF-FF-FF-FF-FF

Delete Revert

DISPLAYING SECURE MAC ADDRESS INFORMATION

Use the Security > Network Access (Show Information) page to display the authenticated MAC addresses stored in the secure MAC address table. Information on the secure MAC entries can be displayed and selected entries can be removed from the table.

CLI REFERENCES

- ◆ ["Network Access \(MAC Address Authentication\)" on page 892](#)

PARAMETERS

These parameters are displayed:

- ◆ **Query By** – Specifies parameters to use in the MAC address query.
 - **Sort Key** – Sorts the information displayed based on MAC address, port interface, or attribute.
 - **MAC Address** – Specifies a specific MAC address.
 - **Interface** – Specifies a port interface.
 - **Attribute** – Displays static or dynamic addresses.
- ◆ **Authenticated MAC Address List**
 - **MAC Address** – The authenticated MAC address.
 - **Interface** – The port interface associated with a secure MAC address.
 - **RADIUS Server** – The IP address of the RADIUS server that authenticated the MAC address.
 - **Time** – The time when the MAC address was last authenticated.
 - **Attribute** – Indicates a static or dynamic address.

WEB INTERFACE

To display the authenticated MAC addresses stored in the secure MAC address table:

1. Click Security, Network Access.
2. Select Show Information from the Step list.
3. Use the sort key to display addresses based MAC address, interface, or attribute.
4. Restrict the displayed addresses by entering a specific address in the MAC Address field, specifying a port in the Interface field, or setting the address type to static or dynamic in the Attribute field.
5. Click Query.

Figure 178: Showing Addresses Authenticated for Network Access

Security > Network Access

Step: 4. Show Information

Query by:

Sort Key: MAC Address

☐ MAC Address

☐ Interface

☐ Attribute

Query

Authenticated MAC Address List Total: 8

	MAC Address	Interface	RADIUS Server	Time	Attribute
<input type="checkbox"/>	00-00-86-45-F2-23	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 16m 12s	Dynamic
<input type="checkbox"/>	00-00-E8-5E-E1-DD	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 24s	Dynamic
<input type="checkbox"/>	00-00-E8-81-93-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 40m 32s	Dynamic
<input type="checkbox"/>	00-01-80-31-B8-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 18m 51s	Dynamic
<input type="checkbox"/>	00-01-80-36-95-D8	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 22s	Dynamic
<input type="checkbox"/>	00-01-80-3B-D3-7F	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 22m 28s	Dynamic
<input type="checkbox"/>	00-01-80-3C-3C-19	Unit 2 / Port 23	10.2.2.10	2008y 20m 12d 11h 15m 19s	Dynamic
<input type="checkbox"/>	00-01-80-3C-3E-B3	Unit 2 / Port 23	10.2.2.10	2008y 20m 12d 11h 17m 40s	Dynamic

Delete Revert

CONFIGURING HTTPS

You can configure the switch to enable 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.

CONFIGURING GLOBAL SETTINGS FOR HTTPS Use the Security > HTTPS (Configure Global) page to enable or disable HTTPS and specify the UDP port used for this service.

CLI REFERENCES

- ◆ "Web Server" on page 847

COMMAND USAGE

- ◆ Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port. (HTTP can only be configured through the CLI using the [ip http server](#) command described on [page 848](#).)
- ◆ 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 6.x or above, or Mozilla Firefox 3.6.2/4/5.
- ◆ The following web browsers and operating systems currently support HTTPS:

Table 20: HTTPS System Support

Web Browser	Operating System
Internet Explorer 6.x or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7
Mozilla Firefox 3.6.2/4/5	Windows 2000, Windows XP, Linux

- ◆ To specify a secure-site certificate, see ["Replacing the Default Secure-site Certificate" on page 338](#).



NOTE: Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

PARAMETERS

These parameters are displayed:

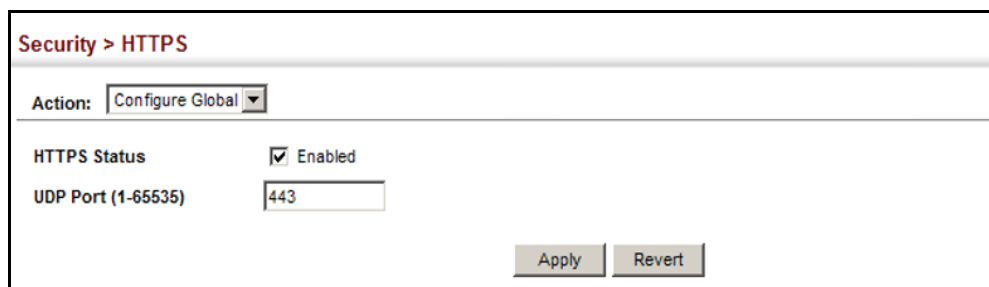
- ◆ **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- ◆ **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

WEB INTERFACE

To configure HTTPS:

1. Click Security, HTTPS.
2. Select Configure Global from the Step list.
3. Enable HTTPS and specify the port number if required.
4. Click Apply.

Figure 179: Configuring HTTPS



Security > HTTPS

Action: Configure Global

HTTPS Status ☒ Enabled

UDP Port (1-65535)

Apply Revert

REPLACING THE DEFAULT SECURE-SITE CERTIFICATE

Use the Security > HTTPS (Copy Certificate) page to replace the default secure-site certificate.

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that the web browser displays will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.



CAUTION: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server and transfer them to the switch to replace the default (unrecognized) certificate with an authorized one.



NOTE: The switch must be reset for the new certificate to be activated. To reset the switch, see ["Resetting the System" on page 147](#) or type "reload" at the command prompt: `Console#reload`

CLI REFERENCES

- ◆ ["Web Server" on page 847](#)

PARAMETERS

These parameters are displayed:

- ◆ **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- ◆ **Certificate Source File Name** – Name of certificate file stored on the TFTP server.

- ◆ **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- ◆ **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.
- ◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

WEB INTERFACE

To replace the default secure-site certificate:

1. Click Security, HTTPS.
2. Select Copy Certificate from the Step list.
3. Fill in the TFTP server, certificate and private key file name, and private password.
4. Click Apply.

Figure 180: Downloading the Secure-Site Certificate

The screenshot shows the 'Security > HTTPS' configuration page. At the top, there is a breadcrumb trail 'Security > HTTPS'. Below it, an 'Action:' dropdown menu is set to 'Copy Certificate'. The main form contains five input fields: 'TFTP Server IP Address' with the value '192.168.0.4', 'Certificate Source File Name' with 'ES3510MA-site-certificate', 'Private Key Source File Name' with 'ES3510MA-private-key', 'Private Password' with masked characters '.....', and 'Confirm Password' also with masked characters '.....'. At the bottom right of the form are two buttons: 'Apply' and 'Revert'.

CONFIGURING THE SECURE SHELL

The Berkeley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkeley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.



NOTE: You need to install an SSH client on the management station to access the switch for management via the SSH protocol.

NOTE: The switch supports both SSH Version 1.5 and 2.0 clients.

COMMAND USAGE

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 on the System Authentication page ([page 307](#)). 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 (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, 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
10825913212890233 76546801726272571413428762941301196195566782
59566410486957427888146206519417467729848654686157177393901647
```



```
79355942303577413098022737087794545240839717526463580581767167
09574804776117
```

3. *Import Client's Public Key to the Switch* – See ["Importing User Public Keys" on page 345](#), or use the `copy tftp public-key` command ([page 736](#)) 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 via the User Accounts page as described on [page 322](#).) 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 Version 1 key:

```
1024 35
13410816856098939210409449201554253476316419218729589211431738
80055536161631051775940838686311092912322268285192543746031009
37187721199696317813662774141689851320491172048303392543241016
37997592371449011938006090253948408482717819437228840253311595
2134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. *Enable SSH Service* – On the SSH Settings page, 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.

CONFIGURING THE SSH SERVER

Use the Security > SSH (Configure Global) page to enable the SSH server and configure basic settings for authentication.



NOTE: A host key pair must be configured on the switch before you can enable the SSH server. See ["Generating the Host Key Pair" on page 344](#).

CLI REFERENCES

- ◆ ["Secure Shell" on page 852](#)

PARAMETERS

These parameters are displayed:

- ◆ **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)

- ◆ **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- ◆ **Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)
- ◆ **Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- ◆ **Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default: 768)
 - 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.

WEB INTERFACE

To configure the SSH server:

1. Click Security, SSH.
2. Select Configure Global from the Step list.
3. Enable the SSH server.
4. Adjust the authentication parameters as required.
5. Click Apply.

Figure 181: Configuring the SSH Server

The screenshot shows a web interface for configuring the SSH server. The breadcrumb is "Security > SSH". The "Step:" dropdown is set to "1. Configure Global". The configuration table is as follows:

Parameter	Value
SSH Server Status	<input checked="" type="checkbox"/> Enabled
Version	2.0
Authentication Timeout (1-120)	120 sec
Authentication Retries (1-5)	3
Server-Key Size (512-896)	768

At the bottom right, there are two buttons: "Apply" and "Revert".

GENERATING THE HOST KEY PAIR

Use the Security > SSH (Configure Host Key - Generate) page to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the section ["Importing User Public Keys" on page 345](#).



NOTE: A host key pair must be configured on the switch before you can enable the SSH server. See ["Configuring the SSH Server" on page 342](#).

CLI REFERENCES

- ◆ ["Secure Shell" on page 852](#)

PARAMETERS

These parameters are displayed:

- ◆ **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both)

The SSH server uses RSA or DSA 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.



NOTE: The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- ◆ **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

WEB INTERFACE

To generate the SSH host key pair:

1. Click Security, SSH.
2. Select Configure Host Key from the Step list.
3. Select Generate from the Action list.
4. Select the host-key type from the drop-down box.
5. Select the option to save the host key from memory to flash if required.
6. Click Apply.

Figure 182: Generating the SSH Host Key Pair

The screenshot shows the 'Security > SSH' configuration page. The 'Step' dropdown is set to '2. Configure Host Key' and the 'Action' dropdown is set to 'Generate'. The 'Host-Key Type' is set to 'Both'. The checkbox 'Save Host-Key from Memory to Flash' is checked. There are 'Apply' and 'Revert' buttons at the bottom right.

To display or clear the SSH host key pair:

1. Click Security, SSH.
2. Select Configure Host Key from the Step list.
3. Select Show from the Action list.
4. Select the host-key type to clear.
5. Click Clear.

Figure 183: Showing the SSH Host Key Pair

The screenshot shows the 'Security > SSH' configuration page with the 'Action' dropdown set to 'Show'. Under the 'Public-Key of Host-Key' section, the 'RSA' checkbox is selected, and the public key is displayed in a text area. The 'DSA' checkbox is also present but not selected. A 'Clear' button is at the bottom right.

Public-Key of Host-Key

☐ RSA

```
1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
732895735202234665421721768844978831196756189309582533
```

☐ DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCriv1ClKmdgE/fi2PqqrYH/ClAB/
sJ1rNAX0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAFQCPzwjn0rSaLiTq53jx1tsj0RILZwAAAIbIL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAc2TmxhjGsEtMlAtxKm+r106pnz2aX9KEzMewJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

Clear

IMPORTING USER PUBLIC KEYS

Use the Security > SSH (Configure User Key - Copy) page to upload a user's public key to the switch. This public key must be stored on the switch for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.

CLI REFERENCES

- ◆ "Secure Shell" on page 852

PARAMETERS

These parameters are displayed:

- ◆ **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page (see ["Configuring User Accounts" on page 322](#)).
- ◆ **User Key Type** – The type of public key to upload.
 - RSA: The switch accepts a RSA version 1 encrypted public key.
 - DSA: The switch accepts a DSA version 2 encrypted public key.

The SSH server uses RSA or DSA 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.

The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- ◆ **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.
- ◆ **Source File Name** – The public key file to upload.

WEB INTERFACE

To copy the SSH user's public key:

1. Click Security, SSH.
2. Select Configure User Key from the Step list.
3. Select Copy from the Action list.
4. Select the user name and the public-key type from the respective drop-down boxes, input the TFTP server IP address and the public key source file name.
5. Click Apply.

Figure 184: Copying the SSH User's Public Key

Security > SSH

Step: 3. Configure User Key Action: Copy

User Name: steve

User-Key Type: RSA

TFTP Server IP Address: 192.168.0.61

Source File Name: rsa.pub

Apply Revert

To display or clear the SSH user's public key:

1. Click Security, SSH.
2. Select Configure User Key from the Step list.
3. Select Show from the Action list.
4. Select a user from the User Name list.
5. Select the host-key type to clear.
6. Click Clear.

Figure 185: Showing the SSH User's Public Key

Security > SSH

Step: 3. Configure User Key Action: Show

User Name: admin

Public-Key of User-Key

☐ RSA

```
1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
732895735202234665421721768844978831196756189309582533
```

☐ DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCriv1ClKmdgE/fiZPqrYH/ClAB/
eJ1rNAX0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAFQCpzwjn0rSaLiTqS3jx1tsj0RILZwAAAIbL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAc2TmxhjGsEtMlAtxKm+rl06pnz2aX9KEzMEwJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

Clear

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, or next header type), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists –

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

COMMAND USAGE

The following restrictions apply to ACLs:

- ◆ The maximum number of ACLs is 512.
- ◆ The maximum number of rules per system is 2048 rules.
- ◆ An ACL can have up to 2048 rules. However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- ◆ The maximum number of rules that can be bound to the ports is 64 for each of the following list types: MAC ACLs, IP ACLs (including Standard and Extended ACLs), IPv6 Standard ACLs, and IPv6 Extended ACLs.

The maximum number of rules (Access Control Entries, or ACEs) stated above is the worst case scenario. In practice, the switch compresses the ACEs in TCAM (a hardware table used to store ACEs), but the actual maximum number of ACEs possible depends on too many factors to be precisely determined. It depends on the amount of hardware resources reserved at runtime for this purpose.

Auto ACE Compression is a software feature used to compress all the ACEs of an ACL to utilize hardware resources more efficiently. Without compression, one ACE would occupy a fixed number of entries in TCAM. So if one ACL includes 25 ACEs, the ACL would need $(25 * n)$ entries in TCAM, where "n" is the fixed number of TCAM entries needed for one ACE. When compression is employed, before writing the ACE into TCAM, the software compresses the ACEs to reduce the number of required TCAM entries. For example, one ACL may include 128 ACEs which classify a continuous IP address range like 192.168.1.0~255. If compression is disabled, the ACL would occupy $(128 * n)$ entries of TCAM, using up nearly all of the hardware resources. When using compression, the 128 ACEs are compressed into one ACE classifying the IP address as 192.168.1.0/24, which requires only "n" entries in TCAM. The above example is an ideal case for compression. The worst case would be if no any ACE can be compressed, in which case the used number of TCAM entries would be the same as without compression. It would also require more time to process the ACEs.

- ◆ If no matches are found down to the end of the list, the traffic is denied. For this reason, frequently hit entries should be placed at the top of the list. There is an implied deny for traffic that is not explicitly permitted. Also, note that a single-entry ACL with only one deny entry has the effect of denying all traffic. You should therefore use at least one permit statement in an ACL or all traffic will be blocked.

Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the packet will be denied.

The order in which active ACLs are checked is as follows:

1. User-defined rules in IP and MAC ACLs for ingress or egress ports are checked in parallel.

2. Rules within an ACL are checked in the configured order, from top to bottom.
3. If the result of checking an IP ACL is to permit a packet, but the result of a MAC ACL on the same packet is to deny it, the packet will be denied (because the decision to deny a packet has a higher priority for security reasons). A packet will also be denied if the IP ACL denies it and the MAC ACL accepts it.

SETTING A TIME RANGE Use the Security > ACL (Configure Time Range) page to sets a time range during which ACL functions are applied.

CLI REFERENCES

- ◆ ["Time Range" on page 776](#)

COMMAND USAGE

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.

PARAMETERS

These parameters are displayed:

Add

- ◆ **Time-Range Name** – Name of a time range. (Range: 1-16 characters)

Add Rule

- ◆ **Time-Range** – Name of a time range.
- ◆ **Mode**
 - **Absolute** – Specifies a specific time or time range.
 - **Start/End** – Specifies the hours, minutes, month, day, and year at which to start or end.
 - **Periodic** – Specifies a periodic interval.
 - **Start/To** – Specifies the days of the week, hours, and minutes at which to start or end.

WEB INTERFACE

To configure a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Add from the Action list.

4. Enter the name of a time range.
5. Click Apply.

Figure 186: Setting the Name of a Time Range

Security > ACL

Step: 1. Configure Time-Range Action: Add

Time-Range Name R&D

Apply Revert

To show a list of time ranges:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show from the Action list.

Figure 187: Showing a List of Time Ranges

Security > ACL

Step: 1. Configure Time-Range Action: Show

Time-Range List Total: 1

	Time-Range Name
<input type="checkbox"/>	R&D

Delete Revert

To configure a rule for a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of time range from the drop-down list.
5. Select a mode option of Absolute or Periodic.
6. Fill in the required parameters for the selected mode.
7. Click Apply.

Figure 188: Add a Rule to a Time Range

Security > ACL

Step: 1. Configure Time-Range Action: Add Rule

Time-Range: R&D

Mode: Periodic

Start

Days of the week: Weekend

Hours (0-23): 5

Minutes (0-59): 30

To

Days of the week: Sunday

Hours (0-23):

Minutes (0-59):

Apply Revert

To show the rules configured for a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show Rule from the Action list.

Figure 189: Showing the Rules Configured for a Time Range

Security > ACL

Step: 1. Configure Time-Range Action: Show Rule

Time-Range: time1

Time-Range Rule List Total: 4

<input type="checkbox"/>	Mode	Start	End
<input type="checkbox"/>	Absolute	2009-01-01 10:05	2010-01-31 20:10
<input type="checkbox"/>	Periodic	Daily 10:05	Daily 20:10
<input type="checkbox"/>	Periodic	Monday 10:05	Tuesday 20:10
<input type="checkbox"/>	Periodic	Monday 00:00	Tuesday 23:59

Delete Revert

SHOWING TCAM UTILIZATION

Use the Security > ACL (Configure ACL - Show TCAM) page to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

CLI REFERENCES

- ◆ ["show access-list tcam-utilization" on page 726](#)

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, QinQ, MAC-based VLANs, VLAN translation, 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.

PARAMETERS

These parameters are displayed:

- ◆ **Total Policy Control Entries** – The number policy control entries in use.
- ◆ **Free Policy Control Entries** – The number of policy control entries available for use.
- ◆ **Entries Used by System** – The number of policy control entries used by the operating system.
- ◆ **Entries Used by User** – The number of policy control entries used by configuration settings, such as access control lists.
- ◆ **TCAM Utilization** – The overall percentage of TCAM in use.

WEB INTERFACE

To show information on TCAM utilization:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show TCAM from the Action list.

Figure 190: Showing TCAM Utilization

Security > ACL	
Step: 2. Configure ACL	Action: Show TCAM
Total Policy Control Entries	3072
Free Policy Control Entries	2884
Entries Used by System	188
Entries Used by User	0
TCAM Utilization	6.11

SETTING THE ACL NAME AND TYPE

Use the Security > ACL (Configure ACL - Add) page to create an ACL.

CLI REFERENCES

- ◆ "access-list ip" on page 950
- ◆ "show ip access-list" on page 955
- ◆ "access-list ipv6" on page 956
- ◆ "show ipv6 access-list" on page 960

PARAMETERS

These parameters are displayed:

- ◆ **ACL Name** – Name of the ACL. (Maximum length: 32 characters)
- ◆ **Type** – The following filter modes are supported:
 - **IP Standard:** IPv4 ACL mode filters packets based on the source IPv4 address.
 - **IP Extended:** IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.
 - **IPv6 Standard:** IPv6 ACL mode filters packets based on the source IPv6 address.
 - **IPv6 Extended:** IPv6 ACL mode filters packets based on the source or destination IP address, as well as DSCP, and the next header type.
 - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).
 - **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection (see ["ARP Inspection" on page 370](#)).

WEB INTERFACE

To configure the name and type of an ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add from the Action list.
4. Fill in the ACL Name field, and select the ACL type.
5. Click Apply.

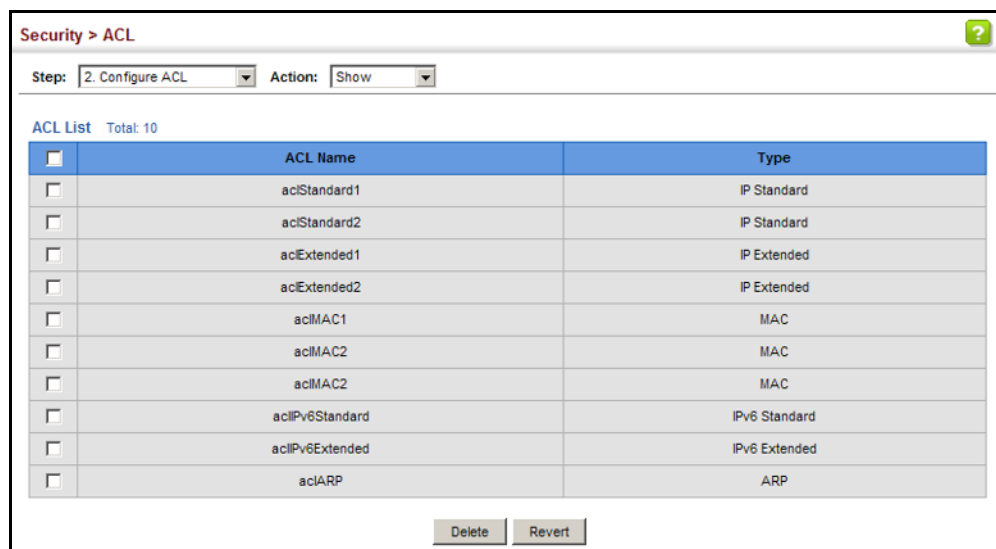
Figure 191: Creating an ACL

The screenshot shows a web interface for configuring an ACL. At the top, it says "Security > ACL". Below this, there are two dropdown menus: "Step:" with "2. Configure ACL" selected, and "Action:" with "Add" selected. Below these, there are two input fields: "ACL Name" with the text "R&D" entered, and "Type" with "IP Standard" selected from a dropdown. At the bottom right, there are two buttons: "Apply" and "Revert".

To show a list of ACLs:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show from the Action list.

Figure 192: Showing a List of ACLs



The screenshot shows the 'Security > ACL' configuration page. At the top, there are two dropdown menus: 'Step: 2. Configure ACL' and 'Action: Show'. Below these, the 'ACL List' is displayed with a 'Total: 10' count. The list is a table with three columns: a checkbox, 'ACL Name', and 'Type'. The ACLs listed are: acStandard1 (IP Standard), acStandard2 (IP Standard), acExtended1 (IP Extended), acExtended2 (IP Extended), acIMAC1 (MAC), acIMAC2 (MAC), acIMAC2 (MAC), acIPv6Standard (IPv6 Standard), acIPv6Extended (IPv6 Extended), and acIARP (ARP). At the bottom right of the table, there are 'Delete' and 'Revert' buttons.

	ACL Name	Type
<input type="checkbox"/>	acStandard1	IP Standard
<input type="checkbox"/>	acStandard2	IP Standard
<input type="checkbox"/>	acExtended1	IP Extended
<input type="checkbox"/>	acExtended2	IP Extended
<input type="checkbox"/>	acIMAC1	MAC
<input type="checkbox"/>	acIMAC2	MAC
<input type="checkbox"/>	acIMAC2	MAC
<input type="checkbox"/>	acIPv6Standard	IPv6 Standard
<input type="checkbox"/>	acIPv6Extended	IPv6 Extended
<input type="checkbox"/>	acIARP	ARP

CONFIGURING A STANDARD IPV4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Standard) page to configure a Standard IPv4 ACL.

CLI REFERENCES

- ◆ "permit, deny (Standard IP ACL)" on page 951
- ◆ "show ip access-list" on page 955
- ◆ "Time Range" on page 776

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source IP Address** – Source IP address.

- ◆ **Source Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- ◆ **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to an IPv4 Standard ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range.
9. Click Apply.

Figure 193: Configuring a Standard IPv4 ACL

The screenshot shows the 'Security > ACL' configuration page. At the top, the 'Step' is set to '2. Configure ACL' and the 'Action' is 'Add Rule'. Under the 'Type' section, 'IP Standard' is selected with a radio button. The 'Name' field is set to 'R&D'. In the 'Action' section, 'Permit' is selected. Under 'Address Type', 'Host' is selected. The 'Source IP Address' field contains '10.1.1.21' and the 'Source Subnet Mask' field contains '255.255.255.255'. The 'Time-Range' checkbox is checked, and the 'Time-Range' dropdown is set to 'R&D'. At the bottom right, there are 'Apply' and 'Revert' buttons.

CONFIGURING AN EXTENDED IPv4 ACL Use the Security > ACL (Configure ACL - Add Rule - IP Extended) page to configure an Extended IPv4 ACL.

CLI REFERENCES

- ◆ "permit, deny (Extended IPv4 ACL)" on page 952
- ◆ "show ip access-list" on page 955
- ◆ "Time Range" on page 776

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Specifies the source or destination IP address type. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source/Destination IP Address** – Source or destination IP address.
- ◆ **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on [page 354](#).)
- ◆ **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- ◆ **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- ◆ **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: Others)
- ◆ **Service Type** – Packet priority settings based on the following criteria:
 - **Precedence** – IP precedence level. (Range: 0-7)
 - **DSCP** – DSCP priority level. (Range: 0-63)
- ◆ **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- ◆ **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63)

The control bit mask is a decimal number (for an equivalent binary 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, control bit mask 2
- Both SYN and ACK valid, use control-code 18, control bit mask 18
- SYN valid and ACK invalid, use control-code 2, control bit mask 18

◆ **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to an IPv4 Extended ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Extended from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range.
9. Set any other required criteria, such as service type, protocol type, or control code.
10. Click Apply.

Figure 194: Configuring an Extended IPv4 ACL

The screenshot shows the 'Security > ACL' configuration page. The 'Step' is '2. Configure ACL' and the 'Action' is 'Add Rule'. The 'Type' is 'IP Extended'. The 'Name' is 'ipe'. The 'Action' is 'Permit'. The 'Source Address Type' is 'IP'. The 'Source IP Address' is '10.7.1.0'. The 'Source Subnet Mask' is '255.255.255.0'. The 'Destination Address Type' is 'Any'. The 'Destination IP Address' is '0.0.0.0'. The 'Destination Subnet Mask' is '0.0.0.0'. The 'Source Port' and 'Destination Port' are both empty. The 'Source Port Bit Mask' and 'Destination Port Bit Mask' are both empty. The 'Protocol' is 'Others'. The 'Control Code' and 'Control Code Bit Mask' are both empty. The 'Service Type' is 'Precedence (0-7)'. The 'Time-Range' checkbox is unchecked. The 'Apply' and 'Revert' buttons are at the bottom right.

CONFIGURING A STANDARD IPV6 ACL

Use the Security > ACL (Configure ACL - Add Rule - IPv6 Standard) page to configure a Standard IPv6 ACL.

CLI REFERENCES

- ◆ "permit, deny (Standard IPv6 ACL)" on page 957
- ◆ "show ipv6 access-list" on page 960
- ◆ "Time Range" on page 776

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IPv6-Prefix" to specify a range of addresses. (Options: Any, Host, IPv6-Prefix; Default: Any)
- ◆ **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.
- ◆ **Source 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 bits)

- ◆ **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to a Standard IPv6 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IPv6 Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the source address type (Any, Host, or IPv6-prefix).
8. If you select "Host," enter a specific address. If you select "IPv6-prefix," enter a subnet address and the prefix length.
9. Click Apply.

Figure 195: Configuring a Standard IPv6 ACL

The screenshot shows the 'Security > ACL' configuration page. At the top, the 'Step' is set to '2. Configure ACL' and the 'Action' is 'Add Rule'. Under the 'Type' section, 'IPv6 Standard' is selected with a radio button. The 'Name' field is set to 'R&D#6S'. In the 'Action' section, 'Permit' is selected from a dropdown. Under 'Source Address Type', 'Host' is selected from a dropdown. The 'Source IPv6 Address' field contains '2009:DB9:2229::79'. The 'Source Prefix Length (0-128)' field contains '128'. There is an unchecked checkbox for 'Time-Range' and a dropdown set to 'R&D'. At the bottom right are 'Apply' and 'Revert' buttons.

CONFIGURING AN EXTENDED IPv6 ACL Use the Security > ACL (Configure ACL - Add Rule - IPv6 Extended) page to configure an Extended IPv6 ACL.

CLI REFERENCES

- ◆ "permit, deny (Extended IPv6 ACL)" on page 958
- ◆ "show ipv6 access-list" on page 960
- ◆ "Time Range" on page 776

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Specifies the source or destination IP address type. Use "Any" to include all possible addresses, or "IPv6-Prefix" to specify a range of addresses. (Options: Any, IPv6-Prefix; Default: Any)
- ◆ **Source/Destination IPv6 Address** – An IPv6 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.
- ◆ **Source/Destination 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 bits for the source address; 0-8 bits for the destination address)
- ◆ **DSCP** – DSCP traffic class. (Range: 0-63)
- ◆ **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

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, and includes 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)
- 50 : Encapsulating Security Payload (RFC 2406)
- 51 : Authentication (RFC 2402)
- 60 : Destination Options (RFC 2460)

WEB INTERFACE

To add rules to an Extended IPv6 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IPv6 Extended from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any or IPv6-prefix).
8. If you select "Host," enter a specific address. If you select "IPv6-prefix," enter a subnet address and prefix length.
9. Set any other required criteria, such as DSCP or next header type.
10. Click Apply.

Figure 196: Configuring an Extended IPv6 ACL

The screenshot shows the 'Security > ACL' configuration page. The 'Step' is set to '2. Configure ACL' and the 'Action' is 'Add Rule'. Under the 'Type' section, 'IPv6 Extended' is selected. The 'Name' is 'ipv6e'. The 'Action' is 'Permit'. The 'Source Address Type' is 'IPv6-Prefix'. The 'Source IPv6 Address' is '2009:DB9:2229:79' and the 'Source Prefix Length (0-128)' is '8'. The 'Destination Address Type' is 'Any'. The 'Destination IPv6 Address' is '::' and the 'Destination Prefix Length (0-8)' is '0'. The 'DSCP (0-63)' and 'Next-Header (0-255)' fields are empty. The 'Time-Range' checkbox is unchecked, and the 'R&D' dropdown is set to 'R&D'. The 'Apply' and 'Revert' buttons are at the bottom right.

Security > ACL	
Step:	2. Configure ACL
Action:	Add Rule
Type	<input type="radio"/> IP Standard <input type="radio"/> IP Extended <input type="radio"/> MAC <input type="radio"/> IPv6 Standard <input checked="" type="radio"/> IPv6 Extended <input type="radio"/> ARP
Name	ipv6e
Action	Permit
Source Address Type	IPv6-Prefix
Source IPv6 Address	2009:DB9:2229:79
Source Prefix Length (0-128)	8
Destination Address Type	Any
Destination IPv6 Address	::
Destination Prefix Length (0-8)	0
DSCP (0-63)	
Next-Header (0-255)	
<input type="checkbox"/> Time-Range	R&D
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

CONFIGURING A MAC ACL Use the Security > ACL (Configure ACL - Add Rule - MAC) page to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

CLI REFERENCES

- ◆ "permit, deny (MAC ACL)" on page 963
- ◆ "show ip access-list" on page 955
- ◆ "Time Range" on page 776

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)
- ◆ **Source/Destination MAC Address** – Source or destination MAC address.
- ◆ **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- ◆ **Packet Format** – This attribute includes the following packet types:
 - **Any** – Any Ethernet packet type.
 - **Untagged-eth2** – Untagged Ethernet II packets.
 - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
 - **Tagged-eth2** – Tagged Ethernet II packets.
 - **Tagged-802.3** – Tagged Ethernet 802.3 packets.
- ◆ **VID** – VLAN ID. (Range: 1-4094)
- ◆ **VID Bit Mask** – VLAN bit mask. (Range: 0-4095)
- ◆ **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 0-ffff hex.)

A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- ◆ **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 0-ffff hex)
- ◆ **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to a MAC ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select MAC from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or MAC).
8. If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexadecimal bit mask for an address range.
9. Set any other required criteria, such as VID, Ethernet type, or packet format.
10. Click Apply.

Figure 197: Configuring a MAC ACL

The screenshot displays the 'Security > ACL' configuration page. At the top, the 'Step' is set to '2. Configure ACL' and the 'Action' is 'Add Rule'. Below this, the 'Type' is set to 'MAC' (selected with a radio button). The 'Name' is 'R&D#3'. The 'Action' is set to 'Permit'. The 'Source Address Type' is 'Any', and the 'Destination Address Type' is 'Any'. The 'Source MAC Address' and 'Destination MAC Address' are both '00-00-00-00-00-00'. The 'Source Bit Mask' and 'Destination Bit Mask' are both '00-00-00-00-00-00'. The 'Packet Format' is 'Any'. The 'VID (1-4094)' is '12' and the 'VID Bit Mask (0-4095)' is '4095'. The 'Ethernet Type' and 'Ethernet Type Bit Mask' are both empty, with a note '(0000-FFFF, hexadecimal value)'. There is a checkbox for 'Time-Range' which is unchecked, and a dropdown menu next to it showing 'rd'. At the bottom right, there are 'Apply' and 'Revert' buttons.

CONFIGURING AN ARP ACL Use the Security > ACL (Configure ACL - Add Rule - ARP) page to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic (see ["Configuring Global Settings for ARP Inspection" on page 371](#)).

CLI REFERENCES

- ◆ ["permit, deny \(ARP ACL\)" on page 968](#)
- ◆ ["show ip access-list" on page 955](#)
- ◆ ["Time Range" on page 776](#)

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Packet Type** – Indicates an ARP request, ARP response, or either type. (Range: IP, Request, Response; Default: IP)
- ◆ **Source/Destination IP Address Type** – Specifies the source or destination IPv4 address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source/Destination IP Address** – Source or destination IP address.
- ◆ **Source/Destination IP Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on [page 354](#).)
- ◆ **Source/Destination MAC Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)
- ◆ **Source/Destination MAC Address** – Source or destination MAC address.
- ◆ **Source/Destination MAC Bit Mask** – Hexadecimal mask for source or destination MAC address.
- ◆ **Log** – Logs a packet when it matches the access control entry.

WEB INTERFACE

To add rules to an ARP ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select ARP from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the packet type (Request, Response, All).
8. Select the address type (Any, Host, or IP).
9. If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "IP," enter a base address and a hexadecimal bit mask for an address range.
10. Enable logging if required.
11. Click Apply.

Figure 198: Configuring a ARP ACL

The screenshot displays the 'Security > ACL' configuration page. At the top, the 'Step' is set to '2. Configure ACL' and the 'Action' is 'Add Rule'. Below this, the 'Type' is set to 'ARP' (indicated by a radio button). The 'Name' field contains 'R&F#7ARP'. The 'Action' dropdown is set to 'Permit'. The 'Packet Type' dropdown is set to 'IP'. The 'Source IP Address Type' is set to 'Any', and the 'Destination IP Address Type' is also set to 'Any'. The 'Source IP Address' and 'Destination IP Address' fields both contain '0.0.0.0'. The 'Source IP Subnet Mask' and 'Destination IP Subnet Mask' fields both contain '0.0.0.0'. The 'Source MAC Address Type' is set to 'Any', and the 'Destination MAC Address Type' is also set to 'Any'. The 'Source MAC Address' and 'Destination MAC Address' fields both contain '00-00-00-00-00-00'. The 'Source MAC Bit Mask' and 'Destination MAC Bit Mask' fields both contain '00-00-00-00-00-00'. There is a 'Log' checkbox which is currently unchecked. At the bottom right, there are 'Apply' and 'Revert' buttons.

BINDING A PORT TO AN ACCESS CONTROL LIST After configuring ACLs, use the Security > ACL (Configure Interface) page to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

CLI REFERENCES

- ◆ "ip access-group" on page 954
- ◆ "show ip access-group" on page 955
- ◆ "mac access-group" on page 965
- ◆ "show mac access-group" on page 966
- ◆ "Time Range" on page 776

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to bind to a port.
- ◆ **Port** – Port identifier.
- ◆ **ACL** – ACL used for ingress or egress packets.
- ◆ **Time Range** – Name of a time range.
- ◆ **Counter** – Enables counter for ACL statistics.

WEB INTERFACE

To bind an ACL to a port:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select IP, MAC or IPv6 from the Type list.
4. Select a port.
5. Select the name of an ACL from the ACL list.
6. Click Apply.

Figure 199: Binding a Port to an ACL

The screenshot shows the 'Security > ACL' configuration page, specifically Step 3: Configure Interface. The 'Type' is set to IP. The 'Port' is set to 1. Under the 'Ingress' section, the 'ACL' checkbox is checked and set to 'ips', 'Time-Range' is unchecked and set to 'R&D', and 'Counter' is unchecked. Under the 'Egress' section, 'ACL' is unchecked and set to 'ips', 'Time-Range' is unchecked and set to 'R&D', and 'Counter' is unchecked. 'Apply' and 'Revert' buttons are at the bottom right.

CONFIGURING ACL MIRRORING

After configuring ACLs, use the Security > ACL > Configure Interface (Add Mirror) page to mirror traffic matching an ACL from one or more source ports to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source VLAN(s) in a completely unobtrusive manner.

CLI REFERENCES

- ◆ ["Local Port Mirroring Commands" on page 1013](#)

COMMAND USAGE

ACL-based mirroring is only used for ingress traffic. To mirror an ACL, follow these steps:

1. Create an ACL as described in the preceding sections.
2. Add one or more mirrored ports to ACL as described under ["Binding a Port to an Access Control List" on page 366](#).
3. Use the Add Mirror page to specify the ACL and the destination port to which matching traffic will be mirrored.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier.
- ◆ **ACL** – ACL used for ingress packets.

WEB INTERFACE

To bind an ACL to a port:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select Add Mirror from the Action list.
4. Select a port.
5. Select the name of an ACL from the ACL list.
6. Click Apply.

Figure 200: Configuring ACL Mirroring

The screenshot shows the 'Security > ACL' configuration page. At the top, there's a breadcrumb 'Security > ACL'. Below it, the 'Step' is set to '3. Configure Interface' and the 'Action' is 'Add Mirror'. There are two dropdown menus: 'Port' with '1' selected and 'ACL' with 'ips' selected. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the ACLs to be mirrored:

1. Select Configure Interface from the Step list.
2. Select Show Mirror from the Action list.
3. Select a port.

Figure 201: Showing the VLANs to Mirror

The screenshot shows the 'Security > ACL' configuration page with the 'Action' set to 'Show Mirror'. The 'Port' dropdown is set to '1'. Below the dropdowns, there's a section titled 'ACL Mirror List' with 'Total: 1'. It contains a table with one row for the 'ips' ACL. The table has a checkbox column and a 'Source Access-List' column. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Source Access-List
<input type="checkbox"/>	ips

SHOWING ACL HARDWARE COUNTERS Use the Security > ACL > Configure Interface (Show Hardware Counters) page to show statistics for ACL hardware counters.

CLI REFERENCES

- ◆ "show access-list" on page 970
- ◆ "clear access-list hardware counters" on page 970

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Type** – Selects the type of ACL.
- ◆ **Direction** – Displays statistics for ingress or egress traffic.
- ◆ **Query** – Displays statistics for selected criteria.
- ◆ **ACL Name** – The ACL bound this port.
- ◆ **Action** – Shows if action is to permit or deny specified packets.
- ◆ *Rules* – Shows the rules for the ACL bound to this port.
- ◆ **Hit** – Shows the number of packets matching this ACL.¹²
- ◆ **Clear Counter** – Clears the hit counter for the specified ACL.

WEB INTERFACE

To show statistics for ACL hardware counters:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select Show Hardware Counters from the Action list.
4. Select a port.
5. Select ingress or egress traffic.

12. Due to a hardware limitation, statistics are only displayed for permit rules.

Figure 202: Showing ACL Statistics

The screenshot shows the 'Security > ACL' configuration page. At the top, there's a breadcrumb 'Security > ACL' and a help icon. Below it, 'Step: 3. Configure Interface' and 'Action: Show Hardware Counter' are displayed. The configuration fields include 'Port' (1), 'Type' (IP Standard), and 'Direction' (Ingress). A 'Query' button is present. Below the fields, 'ACL Name' is 'rd'. A 'Total: 1' label is shown. A table displays the ACL statistics:

Action	Source IP Address	Time-Range	Hit	Clear Counter
Permit	Any		14	Clear

ARP INSPECTION

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP 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. Invalid ARP packets are dropped.

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 (see ["DHCP Snooping Configuration" on page 404](#)). This database is built by DHCP snooping if it is enabled on globally on the switch and on the required VLANs. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured addresses (see ["Configuring an ARP ACL" on page 364](#)).

COMMAND USAGE

Enabling & Disabling ARP Inspection

- ◆ ARP Inspection is controlled on a global and VLAN basis.
- ◆ By default, ARP Inspection is disabled both globally and on all VLANs.
 - If ARP Inspection is globally enabled, then it becomes active only on the VLANs where it has been enabled.
 - When ARP Inspection is enabled globally, all ARP request and reply packets on inspection-enabled VLANs are redirected to the CPU and their switching behavior handled by the ARP Inspection engine.
 - If ARP Inspection is disabled globally, then it becomes inactive for all VLANs, including those where inspection is enabled.

- When ARP Inspection is disabled, all ARP request and reply packets will bypass the ARP Inspection engine and their switching behavior will match that of all other packets.
 - Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration of 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 enabled globally again.
- ◆ The ARP Inspection engine in the current firmware version does not support ARP Inspection on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection (Configure General) page to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.

CLI REFERENCES

- ◆ ["ARP Inspection" on page 934](#)

COMMAND USAGE

ARP Inspection Validation

- ◆ By default, ARP Inspection Validation is disabled.
- ◆ Specifying at least one of the following validations enables ARP Inspection Validation globally. Any combination of the following checks can be active concurrently.
 - Destination 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. These 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.
 - Source 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.

ARP Inspection Logging

- ◆ By default, logging is active for ARP Inspection, and cannot be disabled.
- ◆ The administrator can configure the log facility rate.
- ◆ When the switch drops a packet, it places an entry in the log buffer, then generates a system message on a rate-controlled basis. After the system message is generated, the entry is cleared from the log buffer.
- ◆ Each log 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.
- ◆ If the log buffer is full, the oldest entry will be replaced with the newest entry.

PARAMETERS

These parameters are displayed:

- ◆ **ARP Inspection Status** – Enables ARP Inspection globally.
(Default: Disabled)
- ◆ **ARP Inspection Validation** – Enables extended ARP Inspection Validation if any of the following options are enabled.
(Default: Disabled)
 - **Dst-MAC** – Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
 - **IP** – Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
 - **Src-MAC** – Validates 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.
- ◆ **Log Message Number** – The maximum number of entries saved in a log message. (Range: 0-256; Default: 5)
- ◆ **Log Interval** – The interval at which log messages are sent.
(Range: 0-86400 seconds; Default: 1 second)

WEB INTERFACE

To configure global settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure General from the Step list.
3. Enable ARP inspection globally, enable any of the address validation options, and adjust any of the logging parameters if required.
4. Click Apply.

Figure 203: Configuring Global Settings for ARP Inspection

Security > ARP Inspection

Step: 1. Configure General

ARP Inspection Status ☒ Enabled

ARP Inspection Validate ☒ Dst-MAC ☐ IP ☐ Src-MAC

Log Message Number (0-256) 50

Log Interval (0-86400) 100 sec

Apply Revert

CONFIGURING VLAN SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection (Configure VLAN) page to enable ARP inspection for any VLAN and to specify the ARP ACL to use.

CLI REFERENCES

- ◆ ["ARP Inspection" on page 934](#)

COMMAND USAGE

ARP Inspection VLAN Filters (ACLs)

- ◆ By default, no ARP Inspection ACLs are configured and the feature is disabled.
- ◆ ARP Inspection ACLs are configured within the ARP ACL configuration page (see [page 364](#)).
- ◆ ARP Inspection ACLs can be applied to any configured VLAN.
- ◆ ARP Inspection uses the DHCP snooping bindings database for the list of valid IP-to-MAC address bindings. ARP ACLs take precedence over entries in the DHCP snooping bindings database. The switch first compares ARP packets to any specified ARP ACLs.
- ◆ If *Static* is specified, ARP packets are only validated against the selected ACL – packets are filtered according to any matching rules, packets not matching any rules are dropped, and the DHCP snooping bindings database check is bypassed.

- ◆ If *Static* is not specified, ARP packets are first validated against the selected ACL; if no ACL rules match the packets, then the DHCP snooping bindings database determines their validity.

PARAMETERS

These parameters are displayed:

- ◆ **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)
- ◆ **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)
- ◆ **ARP Inspection ACL Name**
 - *ARP ACL* – Allows selection of any configured ARP ACLs. (Default: None)
 - **Static** – When an ARP ACL is selected, and static mode also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)

WEB INTERFACE

To configure VLAN settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure VLAN from the Step list.
3. Enable ARP inspection for the required VLANs, select an ARP ACL filter to check for configured addresses, and select the Static option to bypass checking the DHCP snooping bindings database if required.
4. Click Apply.

Figure 204: Configuring VLAN Settings for ARP Inspection

The screenshot shows a web interface for configuring ARP Inspection. The breadcrumb is "Security > ARP Inspection". Below it is a "Step:" dropdown menu set to "2. Configure VLAN". The configuration area contains three settings: "ARP Inspection VLAN ID" with a dropdown menu showing "1"; "ARP Inspection VLAN Status" with a checked checkbox and the label "Enabled"; and "ARP Inspection ACL Name" with a checked checkbox, a dropdown menu showing "aaa", and an unchecked checkbox labeled "Static". At the bottom right are "Apply" and "Revert" buttons.

**CONFIGURING
INTERFACE SETTINGS
FOR ARP INSPECTION**

Use the Security > ARP Inspection (Configure Interface) page to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

CLI REFERENCES

- ◆ ["ARP Inspection" on page 934](#)

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or trunk identifier.
- ◆ **Trust Status** – Configures the port as trusted or untrusted.
(Default: Untrusted)

By default, all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting.

Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while those arriving on untrusted interfaces are subject to all configured ARP inspection tests.
- ◆ **Packet Rate Limit** – Sets the maximum number of ARP packets that can be processed by CPU per second on trusted or untrusted ports.
(Range: 0-2048; Default: 15)

Setting the rate limit to "0" means that there is no restriction on the number of ARP packets that can be processed by the CPU.

The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.

WEB INTERFACE

To configure interface settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure Interface from the Step list.
3. Specify any untrusted ports which require ARP inspection, and adjust the packet inspection rate.
4. Click Apply.

Figure 205: Configuring Interface Settings for ARP Inspection

Security > ARP Inspection

Step: 3. Configure Interface

Interface: ☒ Port ☐ Trunk

Port Configuration List Total: 28

Port	Trust Status	Packet Rate Limit (0-2048 pps)
1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> 15
2	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> 15
3	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> 15
4	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> 15
5	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> 15

DISPLAYING ARP INSPECTION STATISTICS

Use the Security > ARP Inspection (Show Information - Show Statistics) page to display statistics about the number of ARP packets processed, or dropped for various reasons.

CLI REFERENCES

- ◆ ["show ip arp inspection statistics" on page 942](#)

PARAMETERS

These parameters are displayed:

Table 21: ARP Inspection Statistics

Parameter	Description
Received ARP packets before ARP inspection rate limit	Count of ARP packets received but not exceeding the ARP Inspection rate limit.
Dropped ARP packets in the process of ARP inspection rate limit	Count of ARP packets exceeding (and dropped by) ARP rate limiting.
ARP packets dropped by additional validation (IP)	Count of ARP packets that failed the IP address test.
ARP packets dropped by additional validation (Dst-MAC)	Count of packets that failed the destination MAC address test.
Total ARP packets processed by ARP inspection	Count of all ARP packets processed by the ARP Inspection engine.
ARP packets dropped by additional validation (Src-MAC)	Count of packets that failed the source MAC address test.
ARP packets dropped by ARP ACLs	Count of ARP packets that failed validation against ARP ACL rules.
ARP packets dropped by DHCP snooping	Count of packets that failed validation against the DHCP Snooping Binding database.

WEB INTERFACE

To display statistics for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Show Information from the Step list.
3. Select Show Statistics from the Action list.

Figure 206: Displaying Statistics for ARP Inspection

Security > ARP Inspection	
Step: 4. Show Information	Action: Show Statistics
Received ARP packets before ARP inspection rate limit	1000
Dropped ARP packets in processing ARP inspection rate limit	5
Total ARP packets processed by ARP inspection	200
ARP packets dropped by additional validation (Src-MAC)	300
ARP packets dropped by additional validation (Dst-MAC)	2000
ARP packets dropped by additional validation (IP)	100
ARP packets dropped by ARP ACLs	5
ARP packets dropped by DHCP snooping	5

DISPLAYING THE ARP INSPECTION LOG

Use the Security > ARP Inspection (Show Information - Show Log) page to show information about entries stored in the log, including the associated VLAN, port, and address components.

CLI REFERENCES

- ◆ ["show ip arp inspection log" on page 942](#)

PARAMETERS

These parameters are displayed:

Table 22: ARP Inspection Log

Parameter	Description
VLAN ID	The VLAN where this packet was seen.
Port	The port where this packet was seen.
Src. IP Address	The source IP address in the packet.
Dst. IP Address	The destination IP address in the packet.
Src. MAC Address	The source MAC address in the packet.
Dst. MAC Address	The destination MAC address in the packet.

WEB INTERFACE

To display the ARP Inspection log:

1. Click Security, ARP Inspection.
2. Select Show Information from the Step list.
3. Select Show Log from the Action list.

Figure 207: Displaying the ARP Inspection Log

Security > ARP Inspection

Step: 4. Show Information Action: Show Log

ARP Inspection Log List Total: 2

VLAN ID	Port	Src. IP Address	Dst. IP Address	Src. MAC Address	Dst. MAC Address
1	15	192.168.1.1	192.168.1.5	11-22-33-44-55-66	AA-BB-CC-DD-EE-FF
1	17	192.168.1.3	192.168.1.23	11-4E-33-75-55-BB	A0-3B-C9-DD-4E-1F

FILTERING IP ADDRESSES FOR MANAGEMENT ACCESS

Use the Security > IP Filter page to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

CLI REFERENCES

- ◆ ["Management IP Filter" on page 877](#)

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 reenter the addresses.

- ◆ You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

PARAMETERS

These parameters are displayed:

◆ **Mode**

- **Web** – Configures IP address(es) for the web group.
- **SNMP** – Configures IP address(es) for the SNMP group.
- **Telnet** – Configures IP address(es) for the Telnet group.
- **All** – Configures IP address(es) for all groups.

- ◆ **Start IP Address** – A single IP address, or the starting address of a range.

- ◆ **End IP Address** – The end address of a range.

WEB INTERFACE

To create a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Add from the Action list.
3. Select the management interface to filter (Web, SNMP, Telnet, All).
4. Enter the IP addresses or range of addresses that are allowed management access to an interface.
5. Click Apply

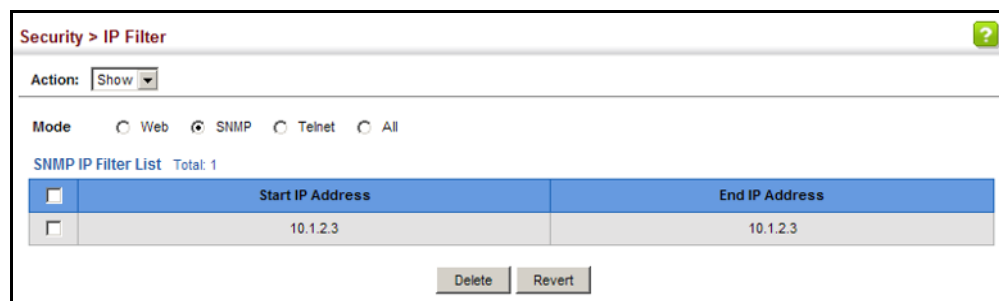
Figure 208: Creating an IP Address Filter for Management Access

The screenshot shows a web interface titled "Security > IP Filter". At the top, there is a section labeled "Action:" with a dropdown menu set to "Add". Below this, there is a "Mode" section with four radio buttons: "Web" (selected), "SNMP", "Telnet", and "All". Underneath the mode selection, there are two text input fields: "Start IP Address" containing the value "10.1.2.3" and "End IP Address" which is currently empty. At the bottom right of the form, there are two buttons: "Apply" and "Revert".

To show a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Show from the Action list.

Figure 209: Showing IP Addresses Authorized for Management Access



CONFIGURING PORT SECURITY

Use the Security > Port Security page to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

When port security is enabled on a port, 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 address table will be authorized to access the network through that 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.

CLI REFERENCES

- ◆ "Port Security" on page 888

COMMAND USAGE

- ◆ The default maximum number of MAC addresses allowed on a secure port is zero (that is, disabled). To use port security, you must configure the maximum number of addresses allowed on a port.
- ◆ 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. 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.

Note that you can manually add additional secure addresses to a port using the Static Address Table (page 227).

- ◆ When the port security state is changed from enabled to disabled, all dynamically learned entries are cleared from the address table.
- ◆ 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 (shut down) due to a security violation, it must be manually re-enabled from the Interface > Port > General page ([page 151](#)).
- ◆ A secure port has the following restrictions:
 - It cannot be used as a member of a static or dynamic trunk.
 - It should not be connected to a network interconnection device.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier.
- ◆ **Security Status** – Enables or disables port security on an interface. (Default: Disabled)
- ◆ **Port Status** – The operational status:
 - Secure/Down – Port security is disabled.
 - Secure/Up – Port security is enabled.
 - Shutdown – Port is shut down due to a response to a port security violation.
- ◆ **Action** – Indicates the action to be taken when a port security violation is detected:
 - **None**: No action should be taken. (This is the default.)
 - **Trap**: Send an SNMP trap message.
 - **Shutdown**: Disable the port.
 - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- ◆ **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
The maximum address count is effective when port security is enabled or disabled.
- ◆ **Current MAC Count** – The number of MAC addresses currently associated with this interface.

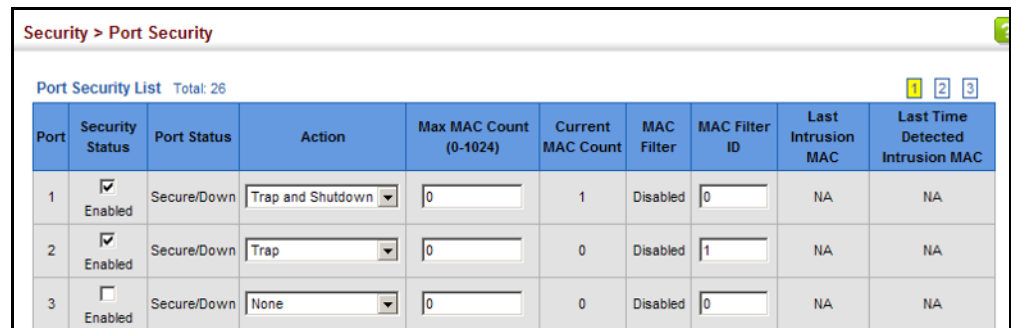
- ◆ **MAC Filter** – Shows if MAC address filtering has been set under Security > Network Access (Configure MAC Filter) as described on [page 333](#).
- ◆ **MAC Filter ID** – The identifier for a MAC address filter.
- ◆ **Last Intrusion MAC** – The last unauthorized MAC address detected.
- ◆ **Last Time Detected Intrusion MAC** – The last time an unauthorized MAC address was detected.

WEB INTERFACE

To configure port security:

1. Click Security, Port Security.
2. Mark the check box in the Security Status column to enable security, set the action to take when an invalid address is detected on a port, and set the maximum number of MAC addresses allowed on the port.
3. Click Apply

Figure 210: Configuring Port Security



The screenshot shows the 'Security > Port Security' web interface. At the top, it says 'Port Security List Total: 26'. Below this is a table with 10 columns: Port, Security Status, Port Status, Action, Max MAC Count (0-1024), Current MAC Count, MAC Filter, MAC Filter ID, Last Intrusion MAC, and Last Time Detected Intrusion MAC. There are three rows of data for ports 1, 2, and 3. Port 1 has Security Status 'Enabled', Port Status 'Secure/Down', Action 'Trap and Shutdown', Max MAC Count '0', Current MAC Count '1', MAC Filter 'Disabled', MAC Filter ID '0', Last Intrusion MAC 'NA', and Last Time Detected Intrusion MAC 'NA'. Port 2 has Security Status 'Enabled', Port Status 'Secure/Down', Action 'Trap', Max MAC Count '0', Current MAC Count '0', MAC Filter 'Disabled', MAC Filter ID '1', Last Intrusion MAC 'NA', and Last Time Detected Intrusion MAC 'NA'. Port 3 has Security Status 'Enabled', Port Status 'Secure/Down', Action 'None', Max MAC Count '0', Current MAC Count '0', MAC Filter 'Disabled', MAC Filter ID '0', Last Intrusion MAC 'NA', and Last Time Detected Intrusion MAC 'NA'.

Port	Security Status	Port Status	Action	Max MAC Count (0-1024)	Current MAC Count	MAC Filter	MAC Filter ID	Last Intrusion MAC	Last Time Detected Intrusion MAC
1	<input checked="" type="checkbox"/> Enabled	Secure/Down	Trap and Shutdown	0	1	Disabled	0	NA	NA
2	<input checked="" type="checkbox"/> Enabled	Secure/Down	Trap	0	0	Disabled	1	NA	NA
3	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA

CONFIGURING 802.1X PORT AUTHENTICATION

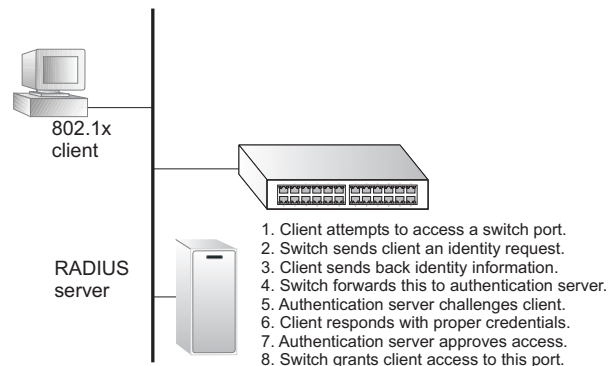
Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access

rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked or assigned to a guest VLAN based on the "intrusion-action" setting. 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.

Figure 211: Configuring Port Security



The operation of 802.1X on the switch requires the following:

- ◆ The switch must have an IP address assigned.
- ◆ RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- ◆ 802.1X must be enabled globally for the switch.
- ◆ Each switch port that will be used must be set to dot1X "Auto" mode.
- ◆ Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- ◆ The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)

- ◆ The RADIUS server and client also have to support the same EAP authentication type – MD5, PEAP, TLS, or TTLS. (Native support for these encryption methods is provided in Windows 7, Vista and XP, and in Windows 2000 with Service Pack 4. To support these encryption methods in Windows 95 and 98, you can use the AEGIS dot1x client or other comparable client software)

CONFIGURING 802.1X GLOBAL SETTINGS

Use the Security > Port Authentication (Configure Global) page to configure IEEE 802.1X port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

CLI REFERENCES

- ◆ ["802.1X Port Authentication" on page 862](#)

PARAMETERS

These parameters are displayed:

- ◆ **System Authentication Control** – Sets the global setting for 802.1X. (Default: Disabled)
- ◆ **EAPOL Pass Through** – Passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. (Default: Disabled)

When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, **EAPOL Pass Through** can be enabled to allow the switch to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

When this device is functioning as an edge switch but does not require any attached clients to be authenticated, **EAPOL Pass Through** can be disabled to discard unnecessary EAPOL traffic.

- ◆ **Identity Profile User Name** – The dot1x supplicant user name. (Range: 1-8 characters)
The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see ["Configuring Port Supplicant Settings for 802.1X" on page 389](#)).
- ◆ **Set Password** – Allows the dot1x supplicant password to be entered.
- ◆ **Identity Profile Password** – The dot1x supplicant password used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. (Range: 1-8 characters)
- ◆ **Confirm Profile Password** – This field is used to confirm the dot1x supplicant password.

- ◆ **Default** – Sets all configurable 802.1X global and port settings to their default values.

WEB INTERFACE

To configure global settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Global from the Step list.
3. Enable 802.1X globally for the switch, and configure EAPOL Pass Through if required. Then set the user name and password to use when the switch responds an MD5 challenge from the authentication server.
4. Click Apply

Figure 212: Configuring Global Settings for 802.1X Port Authentication

The screenshot shows the 'Security > Port Authentication' configuration page. At the top, there's a breadcrumb 'Security > Port Authentication' and a 'Step:' dropdown menu set to '1. Configure Global'. Below this, there are several configuration options:

- System Authentication Control**: A checkbox labeled 'Enabled' which is currently unchecked.
- EAPOL Pass Through**: A checkbox labeled 'Enabled' which is currently unchecked.
- Identity Profile User Name**: A text input field containing the value 'admin'.
- Set Password**: A checkbox labeled 'Set Password' which is checked.
- Identity Profile Password**: A password input field with masked characters (dots).
- Confirm Profile Password**: A password input field with masked characters (dots).

At the bottom right, there are two buttons: 'Apply' and 'Revert'. At the bottom left, there is a 'Default' button and a link that says 'Click this button to set 802.1X global/port settings to default values.'

CONFIGURING PORT AUTHENTICATOR SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface – Authenticator) page to configure 802.1X port settings for the switch as the local authenticator. When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

CLI REFERENCES

- ◆ ["802.1X Port Authentication" on page 862](#)

COMMAND USAGE

- ◆ When the switch functions as a local authenticator between supplicant devices attached to the switch and the authentication server, configure the parameters for the exchange of EAP messages between the authenticator and clients on the Authenticator configuration page.

- ◆ When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters on the Configure Global page (see ["Configuring 802.1X Global Settings" on page 384](#)) which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator (see ["Configuring Port Supplicant Settings for 802.1X" on page 389](#)).
- ◆ This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on this configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on this page and enabling the PAE supplicant on the Supplicant configuration page.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port number.
- ◆ **Status** – Indicates if authentication is enabled or disabled on the port. The status is disabled if the control mode is set to Force-Authorized.
- ◆ **Authorized** – Displays the 802.1X authorization status of connected clients.
 - **Yes** – Connected client is authorized.
 - **N/A** – Connected client is not authorized, or port is not connected.
- ◆ **Control Mode** – Sets the authentication mode to one of the following options:
 - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
 - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
 - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- ◆ **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Default: Single-Host)
 - **Single-Host** – Allows only a single host to connect to this port.
 - **Multi-Host** – Allows multiple host to connect to this port.

In this 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.

- **MAC-Based** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

In this 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).

- ◆ **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- ◆ **Max Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- ◆ **Quiet Period** – Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- ◆ **Tx Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

- ◆ **Supplicant Timeout** – Sets the time that a switch port waits for a response to an EAP request from a client before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

This command attribute 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.

- ◆ **Server Timeout** – Sets the time that a switch port waits for a response to an EAP request from an authentication server before re-transmitting an EAP packet. (Default: 0 seconds)

A RADIUS server must be set before the correct operational value of 10 seconds will be displayed in this field. (See "[Configuring Remote Logon Authentication Servers](#)" on page 308.)

- ◆ **Re-authentication Status** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- ◆ **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- ◆ **Re-authentication Max Retries** – 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. (Range: 1-10;
Default: 2)

- ◆ **Intrusion Action** – Sets the port's response to a failed authentication.
 - **Block Traffic** – Blocks all non-EAP traffic on the port. (This is the default setting.)
 - **Guest VLAN** – All traffic for the port is assigned to a guest VLAN. The guest VLAN must be separately configured (See ["Configuring VLAN Groups" on page 196](#)) and mapped on each port (See ["Configuring Network Access for Ports" on page 330](#)).

Supplicant List

- ◆ **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** – Identifier sent in each EAP Success, Failure or Request packet by the Authentication Server.

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).

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Click Authenticator.
4. Modify the authentication settings for each port as required.
5. Click Apply

Figure 213: Configuring Interface Settings for 802.1X Port Authenticator

Security > Port Authentication

Step: 2. Configure Interface

Type: ☒ Authenticator ☐ Supplicant

Port: 1

Status: Disabled

Authorized: ☒ Yes

Control Mode: Force-Authorized

Operation Mode: Single-Host

Max Count (1-1024): 5

Max Request (1-10): 2

Quiet Period (1-65535): 60 sec

Tx Period (1-65535): 30 sec

Supplicant Timeout (1-65535): 30 sec

Server Timeout: 0 sec

Re-authentication Status: ☐ Enabled

Re-authentication Period (1-65535): 3600 sec

Re-authentication Max Retries (1-10): 2

Intrusion Action: Block Traffic

Supplicant List Total: 1

Supplicant	Authenticator PAE State Machine			Backend State Machine			Reauthentication State Machine
	State	Reauth Count	Current Identifier	State	Request Count	Identifier (Server)	State
00-00-00-00-00-00	Initialize	0	0	Initialize	0	0	Initialize

Apply Revert

CONFIGURING PORT SUPPLICANT SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface – Supplicant) page to configure 802.1X port settings for supplicant requests issued from a port to an authenticator on another device. When 802.1X is enabled and the control mode is set to Force-Authorized (see ["Configuring Port Authenticator Settings for 802.1X" on page 385](#)), you need to configure the parameters for the client supplicant process if the client must be authenticated through another device in the network.

CLI REFERENCES

- ◆ ["802.1X Port Authentication" on page 862](#)

COMMAND USAGE

- ◆ When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters on the Configure Global page (see ["Configuring 802.1X Global Settings" on page 384](#)) which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator on this configuration page. When PAE supplicant mode is enabled on a port, it will not respond to dot1x messages meant for an authenticator.
- ◆ This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on the Authenticator configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on that configuration page and enabling the PAE supplicant on the Supplicant configuration page.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port number.
- ◆ **PAE Supplicant** – Enables PAE supplicant mode. (Default: Disabled)
If the attached client must be authenticated through another device in the network, supplicant status must be enabled.
Supplicant status can only be enabled if PAE Control Mode is set to "Force-Authorized" on this port (see ["Configuring Port Authenticator Settings for 802.1X" on page 385](#)).
PAE supplicant status cannot be enabled if a port is a member of trunk or LACP is enabled on the port.
- ◆ **Authentication Period** – The time that a supplicant port waits for a response from the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)
- ◆ **Held Period** – The time that a supplicant port waits before resending its credentials to find a new authenticator. (Range: 1-65535 seconds; Default: 30 seconds)
- ◆ **Start Period** – The time that a supplicant port waits before resending an EAPOL start frame to the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)
- ◆ **Maximum Start** – The maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. (Range: 1-65535; Default: 3)
- ◆ **Authenticated** – Shows whether or not the supplicant has been authenticated.

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Click Supplicant.
4. Modify the supplicant settings for each port as required.
5. Click Apply

Figure 214: Configuring Interface Settings for 802.1X Port Supplicant

The screenshot shows the 'Security > Port Authentication' web interface. The 'Step' dropdown is set to '2. Configure Interface'. Under the 'Type' section, the 'Supplicant' radio button is selected. The 'Port' dropdown is set to '2'. The 'PAE Supplicant' checkbox is checked and labeled 'Enabled'. Below this, there are five input fields for time periods in seconds: 'Authentication Period (1-65535)' is 30, 'Held Period (1-65535)' is 60, 'Start Period (1-65535)' is 30, and 'Maximum Start (1-65535)' is 3. The 'Authenticated' status is set to 'No'. At the bottom right, there are 'Apply' and 'Revert' buttons.

DISPLAYING 802.1X STATISTICS Use the Security > Port Authentication (Show Statistics) page to display statistics for dot1x protocol exchanges for any port.

CLI REFERENCES

- ◆ ["show dot1x" on page 874](#)

PARAMETERS

These parameters are displayed:

Table 23: 802.1X Statistics

Parameter	Description
<i>Authenticator</i>	
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.

Table 23: 802.1X Statistics (Continued)

Parameter	Description
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Authenticator.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
<i>Supplicant</i>	
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Supplicant in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Supplicant.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Supplicant.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Supplicant.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Supplicant.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Supplicant.
Rx EAP LenError	The number of EAPOL frames that have been received by this Supplicant in which the Packet Body Length field is invalid.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Supplicant.
Tx EAPOL Start	The number of EAPOL Start frames that have been transmitted by this Supplicant.
Tx EAPOL Logoff	The number of EAPOL Logoff frames that have been transmitted by this Supplicant.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Supplicant.
Tx EAP Req/Oth	The number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Supplicant.

WEB INTERFACE

To display port authenticator statistics for 802.1X:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Click Authenticator.

Figure 215: Showing Statistics for 802.1X Port Authenticator

Security > Port Authentication

Step: 3. Show Statistics

Type
☒ Authenticator
☐ Supplicant

Port
1

Port Authentication Authenticator Statistics

Rx EAPOL Start	11154	Rx EAP Resp/Id	2533664
Rx EAPOL Logoff	2115542	Rx EAP Resp/Oth	11123
Rx EAPOL Invalid	533	Rx EAP LenError	1
Rx EAPOL Total	1000	Tx EAP Req/Id	5222
Rx Last EAPOLVer	255	Tx EAP Req/Oth	1222
Rx Last EAPOLSrc	00-02-44-51-C2-90	Tx EAPOL Total	1

Refresh

To display port supplicant statistics for 802.1X:

- 1. Click Security, Port Authentication.
- 2. Select Show Statistics from the Step list.
- 3. Click Supplicant.

Figure 216: Showing Statistics for 802.1X Port Supplicant

Security > Port Authentication

Step: 3. Show Statistics

Type ☐ Authenticator ☒ Supplicant

Port 1

Port Authentication Supplicant Statistics

Rx EAPOL Invalid	11154	Rx EAP LenError	2533664
Rx EAPOL Total	2115542	Tx EAPOL Total	11123
Rx Last EAPOLVer	533	Tx EAPOL Start	1
Rx Last EAPOLSrc	1000	Tx EAPOL Logoff	5222
Rx EAP Resp/Id	255	Tx EAP Req/Id	1222
Rx EAP Resp/Oth	00-02-44-51-C2-90	Tx EAP Req/Oth	1

Refresh

DoS PROTECTION

Use the Security > DoS Protection page to protect against denial-of-service (DoS) attacks. A 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 how to protect against DoS attacks.

CLI REFERENCES

- ◆ "Denial of Service Protection" on page 943

PARAMETERS

These parameters are displayed:

- ◆ **Echo/Chargen Attack** – Attacks in which the echo service repeats anything sent to it, and the chargen (character generator) service generates a continuous stream of data. When used together, they create an infinite loop and result in a denial-of-service.
(Default: Disabled)

- ◆ **Echo/Chargen Attack Rate** – Maximum allowed rate.
(Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- ◆ **Smurf Attack** – 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.
(Default: Enabled)
- ◆ **TCP Flooding Attack** – 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. (Default: Disabled)
- ◆ **TCP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- ◆ **TCP Null Scan** – 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.
(Default: Enabled)
- ◆ **TCP-SYN/FIN Scan** – 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. (Default: Enabled)
- ◆ **TCP Xmas Scan** – 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. (Default: Enabled)
- ◆ **UDP Flooding Attack** – 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.
(Default: Disabled)
- ◆ **UDP Flooding Attack Rate** – Maximum allowed rate.
(Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- ◆ **WinNuke Attack** – 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), causing 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. (Default: Disabled)

- ◆ **WinNuke Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)

WEB INTERFACE

To protect against DoS attacks:

1. Click Security, DoS Protection.
2. Enable protection for specific DoS attacks, and set the maximum allowed rate as required.
3. Click Apply

Figure 217: Protecting Against DoS Attacks

The screenshot displays the 'Security > DoS Protection' configuration page. It features a list of attack types with checkboxes for enabling protection and input fields for setting attack rates. The settings are as follows:

Attack Type	Enabled	Attack Rate (kbits/second)
Echo/Chargen Attack	<input type="checkbox"/>	1000
Echo/Chargen Attack Rate (64-2000)		1000
Smurf Attack	<input checked="" type="checkbox"/>	
TCP Flooding Attack	<input type="checkbox"/>	1000
TCP Flooding Attack Rate (64-2000)		1000
TCP Null Scan	<input checked="" type="checkbox"/>	
TCP SYN/FIN Scan	<input checked="" type="checkbox"/>	
TCP Xmas Scan	<input checked="" type="checkbox"/>	
UDP Flooding Attack	<input type="checkbox"/>	1000
UDP Flooding Attack Rate (64-2000)		1000
WinNuke Attack	<input type="checkbox"/>	1000
WinNuke Attack Rate (64-2000)		1000

At the bottom right, there are 'Apply' and 'Revert' buttons.

IP SOURCE GUARD

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see ["DHCP Snooping" on page 402](#)). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands how to use IP Source Guard.

**CONFIGURING PORTS
FOR IP SOURCE
GUARD**

Use the Security > IP Source Guard > Port Configuration page to set the filtering type based on source IP address, or source IP address and MAC address pairs.

IP 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.

CLI REFERENCES

- ◆ ["ip source-guard" on page 931](#)

COMMAND USAGE

- ◆ Setting source guard mode to SIP (Source IP) or SIP-MAC (Source IP and 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. If no matching entry is found, the packet is dropped.



NOTE: Multicast addresses cannot be used by IP Source Guard.

- ◆ When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping (see ["DHCP Snooping" on page 402](#)), or static addresses configured in the source guard binding table.
- ◆ If 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 DHCP snooping is disabled (see [page 404](#)), 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 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 have not yet been configured (neither by static configuration in the IP source guard binding table nor dynamically learned from DHCP snooping), the switch will drop all IP traffic on that port, except for DHCP packets.

PARAMETERS

These parameters are displayed:

- ◆ **Filter Type** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)
 - **None** – Disables IP source guard filtering on the port.
 - **SIP** – Enables traffic filtering based on IP addresses stored in the binding table.
 - **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.
- ◆ **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)

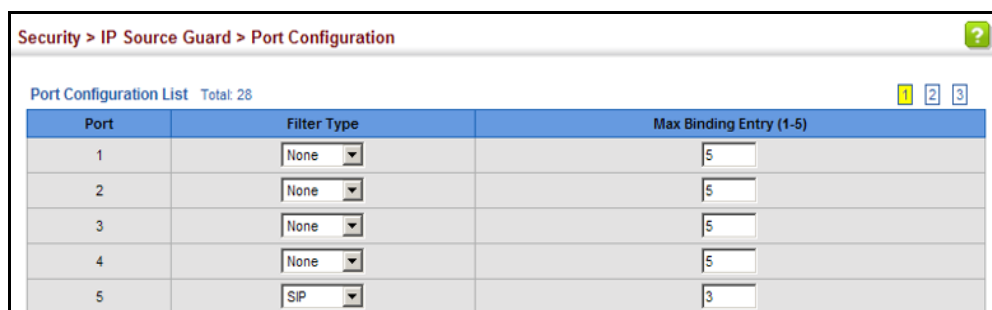
This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping (see ["DHCP Snooping" on page 402](#)) and static entries set by IP source guard (see ["Configuring Static Bindings for IP Source Guard" on page 399](#)).

WEB INTERFACE

To set the IP Source Guard filter for ports:

1. Click Security, IP Source Guard, Port Configuration.
2. Set the required filtering type for each port.
3. Click Apply

Figure 218: Setting the Filter Type for IP Source Guard



Security > IP Source Guard > Port Configuration

Port Configuration List Total: 28

Port	Filter Type	Max Binding Entry (1-5)
1	None	5
2	None	5
3	None	5
4	None	5
5	SIP	3

**CONFIGURING STATIC
BINDINGS FOR IP
SOURCE GUARD**

Use the Security > IP Source Guard > Static Configuration page to bind a static address to a port. Table entries include a MAC address, IP address, lease time, entry type (Static, Dynamic), VLAN identifier, and port identifier. All static entries are configured with an infinite lease time, which is indicated with a value of zero in the table.

CLI REFERENCES

- ◆ ["ip source-guard binding" on page 930](#)

COMMAND USAGE

- ◆ Static addresses entered in the source guard binding table are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- ◆ Static bindings are processed as follows:
 - If there is no entry with the same VLAN ID and MAC address, a new entry is added to the binding table using the type "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.
 - Only unicast addresses are accepted for static bindings.

PARAMETERS

These parameters are displayed:

Add

- ◆ **Port** – The port to which a static entry is bound.
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4093)
- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **IP Address** – A valid unicast IP address, including classful types A, B or C.

Show

- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **Interface** – The port to which this entry is bound.

- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **Lease Time** – The time for which this IP address is leased to the client. (This value is zero for all static addresses.)

WEB INTERFACE

To configure static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.
2. Select Add from the Action list.
3. Enter the required bindings for each port.
4. Click Apply

Figure 219: Configuring Static Bindings for IP Source Guard

Security > IP Source Guard > Static Binding

Action: Add

Port: 1

VLAN: 1

MAC Address: 00-10-B5-F4-00-01

IP Address: 10.2.44.96

Apply Revert

To display static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.
2. Select Show from the Action list.

Figure 220: Displaying Static Bindings for IP Source Guard

Security > IP Source Guard > Static Binding

Action: Show

Static Binding List Total: 1

<input type="checkbox"/>	VLAN	MAC Address	Interface	IP Address	Lease Time (sec)
<input type="checkbox"/>	1	00-10-B5-F4-00-01	Unit 1 / Port 1	192.168.0.23	0

Delete Revert

**DISPLAYING
INFORMATION FOR
DYNAMIC IP SOURCE
GUARD BINDINGS**

Use the Security > IP Source Guard > Dynamic Binding page to display the source-guard binding table for a selected interface.

CLI REFERENCES

- ◆ ["show ip dhcp snooping binding" on page 922](#)

PARAMETERS

These parameters are displayed:

Query by

- ◆ **Port** – A port on this switch.
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4093)
- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **IP Address** – A valid unicast IP address, including classful types A, B or C.

Dynamic Binding List

- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **Interface** – Port to which this entry is bound.
- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **Lease Time** – The time for which this IP address is leased to the client.

WEB INTERFACE

To display the binding table for IP Source Guard:

1. Click Security, IP Source Guard, Dynamic Binding.
2. Mark the search criteria, and enter the required values.
3. Click Query

Figure 221: Showing the IP Source Guard Binding Table

Security > IP Source Guard > Dynamic Binding

Query by:

☐ Port

☐ VLAN

☐ MAC Address

☐ IP Address

Query

Dynamic Binding List Total: 3

VLAN	MAC Address	Interface	IP Address	Lease Time (sec)
1	00-10-B5-F4-00-01	Unit 1 / Port 2	10.2.44.96	5
1	00-10-B5-F4-00-02	Unit 1 / Port 4	10.2.44.97	25
2	00-10-B5-F4-00-03	Unit 1 / Port 7	10.2.44.98	47

DHCP SNOOPING

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

COMMAND USAGE

DHCP Snooping Process

- ◆ 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 a non-secure interface from outside the network or fire wall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.
- ◆ Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- ◆ 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.
- ◆ When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- ◆ Filtering rules are implemented as follows:
 - If the 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 a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
 - If the DHCP packet is not a recognizable type, it is dropped.
 - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
 - If a DHCP packet from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
 - If the 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. 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.

DHCP Snooping Option 82

- ◆ DHCP provides a relay mechanism for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also 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. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.
- ◆ DHCP Snooping must be enabled for Option 82 information to be inserted into request packets.
- ◆ 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. This information may specify the MAC address or IP address of the requesting device (that is, the switch in this context).

By default, the switch also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the port and VLAN ID. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN.
- ◆ If DHCP Snooping Information Option 82 is enabled on the switch, information may be inserted into a DHCP request packet received over any VLAN (depending on DHCP snooping filtering rules). The information inserted into the relayed packets includes the circuit-id and remote-id, as well as the gateway Internet address.
- ◆ 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.

DHCP SNOOPING CONFIGURATION

Use the IP Service > DHCP > Snooping (Configure Global) page to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

CLI REFERENCES

- ◆ ["DHCPv4 Snooping" on page 911](#)

PARAMETERS

These parameters are displayed:

- ◆ **DHCP Snooping Status** – Enables DHCP snooping globally. (Default: Disabled)

- ◆ **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If 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. (Default: Enabled)
- ◆ **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)
- ◆ **DHCP Snooping Information Option Sub-option Format** – Enables or disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information. (Default: Enabled)
- ◆ **DHCP Snooping Information Option Remote ID** – Specifies the MAC address, IP address, or arbitrary identifier of the requesting device (i.e., the switch in this context).
 - **MAC Address** – Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (i.e., the MAC address of the switch's CPU). This attribute can be encoded in Hexadecimal or ASCII.
 - **IP Address** – Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (i.e., the IP address of the management interface). This attribute can be encoded in Hexadecimal or ASCII.
 - *string* – An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)
- ◆ **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.
 - **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. (This is the default policy.)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Configure Global from the Step list.
3. Select the required options for the general DHCP snooping process and for the DHCP Option 82 information option.
4. Click Apply

Figure 222: Configuring Global Settings for DHCP Snooping

The screenshot shows the configuration interface for DHCP Snooping. The breadcrumb trail is 'IP Service > DHCP > Snooping'. The 'Step' dropdown is set to '1. Configure Global'. Under the 'General' section, 'DHCP Snooping Status' is checked (Enabled) and 'DHCP Snooping MAC-Address Verification' is checked (Enabled). Under the 'Information' section, 'DHCP Snooping Information Option Status' is checked (Enabled), 'DHCP Snooping Information Option Sub-option Format' is set to 'Extra Subtype Included', 'DHCP Snooping Information Option Remote ID' is set to 'MAC Address (Hex Encoded)', and 'DHCP Snooping Information Option Policy' is set to 'Replace'. 'Apply' and 'Revert' buttons are at the bottom right.

DHCP SNOOPING VLAN CONFIGURATION

Use the IP Service > DHCP > Snooping (Configure VLAN) page to enable or disable DHCP snooping on specific VLANs.

CLI REFERENCES

- ◆ ["ip dhcp snooping vlan" on page 917](#)

COMMAND USAGE

- ◆ When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- ◆ 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 DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of a configured VLAN. (Range: 1-4093)
- ◆ **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN. (Default: Disabled)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Configure VLAN from the Step list.
3. Enable DHCP Snooping on any existing VLAN.
4. Click Apply

Figure 223: Configuring DHCP Snooping on a VLAN



IP Service > DHCP > Snooping

Step: 2. Configure VLAN

VLAN: 1

DHCP Snooping Status: ☒ Enabled

Apply Revert

CONFIGURING PORTS FOR DHCP SNOOPING

Use the IP Service > DHCP > Snooping (Configure Interface) page to configure switch ports as trusted or untrusted.

CLI REFERENCES

- ◆ ["ip dhcp snooping trust" on page 919](#)

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.
- ◆ When DHCP snooping is enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- ◆ Set all ports connected to DHCP servers within the local network or fire wall to trusted state. Set all other ports outside the local network or fire wall to untrusted state.

PARAMETERS

These parameters are displayed:

- ◆ **Trust Status** – Enables or disables a port as trusted.
(Default: Disabled)
- ◆ **Circuit ID** – Specifies DHCP Option 82 circuit ID suboption information.
 - **Mode** – Specifies the default string “VLAN-Unit-Port” or an arbitrary string. (Default: VLAN-Unit-Port)
 - **Value** – An arbitrary string inserted into the circuit identifier field.
(Range: 1-32 characters)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Configure Interface from the Step list.
3. Set any ports within the local network or firewall to trusted.
4. Specify the mode used for sending circuit ID information, and an arbitrary string if required.
5. Click Apply

Figure 224: Configuring the Port Mode for DHCP Snooping

IP Service > DHCP > Snooping

Step: 3. Configure Interface

Interface: ☒ Port ☐ Trunk

DHCP Snooping Port List Total: 28

Port	Trust Status	Circuit ID	
		Mode	Value
1	<input type="checkbox"/> Enabled	VLAN-Unit-Port	
2	<input type="checkbox"/> Enabled	VLAN-Unit-Port	
3	<input type="checkbox"/> Enabled	VLAN-Unit-Port	
4	<input type="checkbox"/> Enabled	VLAN-Unit-Port	
5	<input checked="" type="checkbox"/> Enabled	String	RD-934

DISPLAYING DHCP SNOOPING BINDING INFORMATION

Use the IP Service > DHCP > Snooping (Show Information) page to display entries in the binding table.

CLI REFERENCES

- ◆ "show ip dhcp snooping binding" on page 922

PARAMETERS

These parameters are displayed:

- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **Lease Time** – The time for which this IP address is leased to the client.
- ◆ **Type** – Entry types include:
 - **DHCP-Snooping** – Dynamically snooped.
 - **Static-DHCPSPNP** – Statically configured.
- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **Interface** – Port or trunk to which this entry is bound.
- ◆ **Store** – Writes all dynamically learned snooping entries to flash memory. This function 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.
- ◆ **Clear** – Removes all dynamically learned snooping entries from flash memory.

WEB INTERFACE

To display the binding table for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Show Information from the Step list.
3. Use the Store or Clear function if required.

Figure 225: Displaying the Binding Table for DHCP Snooping

The screenshot shows the web interface for IP Service > DHCP > Snooping. The 'Step' dropdown is set to '4. Show Information'. Below the dropdown is the title 'DHCP Snooping Binding List Total: 6'. A table displays the binding list with columns: MAC Address, IP Address, Lease Time (seconds), Type, VLAN, and Interface. The table contains 6 rows of data. Below the table are two buttons: 'Store' and 'Clear', each with a descriptive tooltip.

MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface
00-10-B5-F4-00-01	10.2.44.96	5	DHCP-Snooping	1	Trunk 1
00-10-B5-F4-00-02	10.3.44.96	15	Static-DHCPSPNP	1	Unit 1 / Port 2
00-10-B5-F4-00-03	10.4.44.96	25	DHCP-Snooping	1	Unit 1 / Port 3
00-10-B5-F4-00-04	10.5.44.96	10	Static-DHCPSPNP	1	Trunk 4
00-10-B5-F4-00-05	10.6.44.96	10	DHCP-Snooping	1	Unit 1 / Port 5
00-10-B5-F4-00-06	10.7.44.96	5	Static-DHCPSPNP	1	Unit 1 / Port 6

Store Click the button to Store DHCP Snooping binding entries to flash.

Clear Click the button to Clear DHCP Snooping binding entries from flash.

This chapter describes basic administration tasks including:

- ◆ [Event Logging](#) – Sets conditions for logging event messages to system memory or flash memory, configures conditions for sending trap messages to remote log servers, and configures trap reporting to remote hosts using Simple Mail Transfer Protocol (SMTP).
- ◆ [Link Layer Discovery Protocol \(LLDP\)](#) – Configures advertisement of basic information about the local switch, or discovery of information about neighboring devices on the local broadcast domain.
- ◆ [Power over Ethernet](#)¹³ – Sets the priority and power budget for each port.
- ◆ [Simple Network Management Protocol \(SNMP\)](#) – Configures switch management through SNMPv1, SNMPv2c or SNMPv3.
- ◆ [Remote Monitoring \(RMON\)](#) – Configures local collection of detailed statistics or events which can be subsequently retrieved through SNMP.
- ◆ [Switch Clustering](#) – Configures centralized management by a single unit over a group of switches connected to the same local network.
- ◆ [Ethernet Ring Protection Switching \(ERPS\)](#) – Configures a protection switching mechanism and protocol for Ethernet layer network rings.
- ◆ [Connectivity Fault Management \(CFM\)](#) – This protocol provides 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.
- ◆ [Operation, Administration and Maintenance \(OAM\)](#) – Provides remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment).

13. ECS4510-28P/52P

CONFIGURING EVENT LOGGING

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

SYSTEM LOG CONFIGURATION

Use the Administration > Log > System (Configure Global) page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

CLI REFERENCES

- ◆ ["Event Logging" on page 757](#)

PARAMETERS

These parameters are displayed:

- ◆ **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- ◆ **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 24: Logging Levels

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

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- ◆ **RAM Level** – Limits log messages saved to the switch’s temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)



NOTE: The Flash Level must be equal to or less than the RAM Level.

NOTE: All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).

NOTE: 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).

WEB INTERFACE

To configure the logging of error messages to system memory:

1. Click Administration, Log, System.
2. Select Configure Global from the Step list.
3. Enable or disable system logging, set the level of event messages to be logged to flash memory and RAM.
4. Click Apply.

Figure 226: Configuring Settings for System Memory Logs

Administration > Log > System

Step: 1. Configure Global

System Log Status ☒ Enabled

Flash Level 3 - Error

RAM Level 7 - Debugging

Note: The Flash Level must be equal to or less than the RAM Level.

Apply Revert

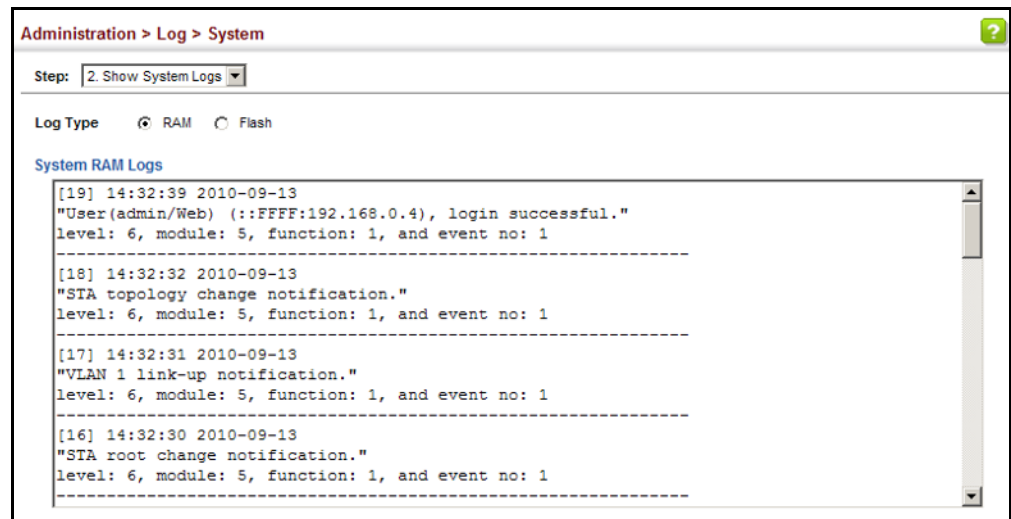
To show the error messages logged to system or flash memory:

1. Click Administration, Log, System.
2. Select Show System Logs from the Step list.
3. Click RAM to display log messages stored in system memory, or Flash to display messages stored in flash memory.

This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary

random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Figure 227: Showing Error Messages Logged to System Memory



REMOTE LOG CONFIGURATION

Use the Administration > Log > Remote page to send log messages to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

CLI REFERENCES

- ◆ ["Event Logging" on page 757](#)

PARAMETERS

These parameters are displayed:

- ◆ **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- ◆ **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

The attribute 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 process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- ◆ **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- ◆ **Server IP Address** – Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.

- ◆ **Port** - Host UDP port to use. (Range: 1-65535; Default: 514)

WEB INTERFACE

To configure the logging of error messages to remote servers:

1. Click Administration, Log, Remote.
2. Enable remote logging, specify the facility type to use for the syslog messages. and enter the IP address of the remote servers.
3. Click Apply.

Figure 228: Configuring Settings for Remote Logging of Error Messages

Administration > Log > Remote

Remote Log Status ☐ Enabled

Logging Facility 23 - Local use 7

Logging Trap Level 0 - System unusable

Server IP Address 1 192.168.0.4 Port 514

Server IP Address 2 Port

Server IP Address 3 Port

Server IP Address 4 Port

Server IP Address 5 Port

Apply Revert

**SENDING SIMPLE MAIL
TRANSFER PROTOCOL
ALERTS**

Use the Administration > Log > SMTP page to alert system administrators of problems by sending SMTP (Simple Mail Transfer Protocol) email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

CLI REFERENCES

- ◆ "SMTP Alerts" on page 763

PARAMETERS

These parameters are displayed:

- ◆ **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- ◆ **Severity** – Sets the syslog severity threshold level (see table on [page 412](#)) used to trigger alert messages. 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. (Default: Level 7)
- ◆ **Email Source Address** – Sets the email address used for the "From" field in alert messages. You may use a symbolic email address that

identifies the switch, or the address of an administrator responsible for the switch.

- ◆ **Email Destination Address** – Specifies the email recipients of alert messages. You can specify up to five recipients.
- ◆ **Server IP Address** – Specifies a list of up to three recipient SMTP servers. IPv4 or IPv6 addresses may be specified. The switch attempts to connect to the listed servers in sequential order if the first server fails to respond.

WEB INTERFACE

To configure SMTP alert messages:

1. Click Administration, Log, SMTP.
2. Enable SMTP, specify a source email address, and select the minimum severity level. Specify the source and destination email addresses, and one or more SMTP servers.
3. Click Apply.

Figure 229: Configuring SMTP Alert Messages

Administration > Log > SMTP

SMTP Status	<input checked="" type="checkbox"/> Enabled
Severity	3 - Error
E-mail Source Address	big-wheels@matel.com
E-mail Destination Address 1	chris@matel.com
E-mail Destination Address 2	
E-mail Destination Address 3	
E-mail Destination Address 4	
E-mail Destination Address 5	
Server IP Address 1	192.168.1.4
Server IP Address 2	
Server IP Address 3	

Apply Revert

LINK LAYER DISCOVERY PROTOCOL

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.

SETTING LLDP TIMING ATTRIBUTES

Use the Administration > LLDP (Configure Global) page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

CLI REFERENCES

- ◆ ["LLDP Commands" on page 1269](#)

PARAMETERS

These parameters are displayed:

- ◆ **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)
- ◆ **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- ◆ **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

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.

TTL in seconds is based on the following rule:
minimum value ((Transmission Interval * Holdtime Multiplier), or 65535)

Therefore, the default TTL is $4 * 30 = 120$ seconds.

- ◆ **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

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 rule:
 $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$

- ◆ **Reinitialization Delay** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

- ◆ **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

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 `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

- ◆ **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets)

The MED Fast Start Count 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.

WEB INTERFACE

To configure LLDP timing attributes:

1. Click Administration, LLDP.
2. Select Configure Global from the Step list.
3. Enable LLDP, and modify any of the timing parameters as required.
4. Click Apply.

Figure 230: Configuring LLDP Timing Attributes

The screenshot displays the 'Administration > LLDP' configuration page. At the top, a 'Step:' dropdown menu is set to '1. Configure Global'. Below this, the 'LLDP' section is checked and labeled 'Enabled'. A list of timing parameters follows, each with a text input field and a unit indicator:

- Transmission Interval (5-32768): 30 sec
- Hold Time Multiplier (2-10): 4
- Delay Interval (1-8192): 2 sec
- Reinitialization Delay (1-10): 2 sec
- Notification Interval (5-3600): 5 sec
- MED Fast Start Count (1-10): 4

A blue note at the bottom states: 'Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.' At the bottom right, there are 'Apply' and 'Revert' buttons.

CONFIGURING LLDP INTERFACE ATTRIBUTES

Use the Administration > LLDP (Configure Interface) page to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

CLI REFERENCES

- ◆ ["LLDP Commands" on page 1269](#)

PARAMETERS

These parameters are displayed:

- ◆ **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)

- ◆ **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Disabled)

This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

For information on defining SNMP trap destinations, see ["Specifying Trap Managers" on page 462](#).

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 `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` notification-events missed due to throttling or transmission loss.

- ◆ **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Disabled)

- ◆ **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.

- **Management Address** – 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 in the performance of 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.

- **Port Description** – 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.
 - **System Capabilities** – 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.
 - **System Description** – 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.
 - **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see ["Displaying System Information" on page 120](#).
- ◆ **802.1 Organizationally Specific TLVs** – Configures IEEE 802.1 information included in the TLV field of advertised messages.
- **Protocol Identity** – The protocols that are accessible through this interface (see ["Protocol VLANs" on page 215](#)).
 - **VLAN ID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see ["IEEE 802.1Q VLANs" on page 193](#)).
 - **VLAN Name** – The name of all VLANs to which this interface has been assigned (see ["IEEE 802.1Q VLANs" on page 193](#)).
 - **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface (see ["Protocol VLANs" on page 215](#)).
- ◆ **802.3 Organizationally Specific TLVs** – Configures IEEE 802.3 information included in the TLV field of advertised messages.
- **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.

- **Max Frame Size** – The maximum frame size. (See ["Configuring Support for Jumbo Frames" on page 122](#) for information on configuring the maximum frame size for this switch
- **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.
- **PoE¹⁴** – Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.
- ◆ **MED TLVs** – Configures general information included in the MED TLV field of advertised messages.
 - **Capabilities** – 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.
 - **Extended Power¹⁴** – This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode).
 - **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
 - **Location** – This option advertises location identification details.
 - **Network Policy** – 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.
- ◆ **MED-Location Civic Address** – Configures information for the location of the attached device included in the MED TLV field of advertised messages, including the country and the device type.
 - **Country** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)
 - **Device entry refers to** – The type of device to which the location applies:
 - Location of DHCP server.
 - Location of network element closest to client.
 - Location of client. (This is the default.)

14. ECS4510-28P/52P

WEB INTERFACE

To configure LLDP interface attributes:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Configure General from the Action list.
4. Select an interface from the Port or Trunk list.
5. Set the LLDP transmit/receive mode, specify whether or not to send SNMP trap messages, and select the information to advertise in LLDP messages.
6. Click Apply.

Figure 231: Configuring LLDP Interface Attributes

The screenshot shows the 'Administration > LLDP' web interface. The 'Step' is '2. Configure Interface' and the 'Action' is 'Configure General'. The 'Interface' is set to 'Port 1'. The 'Admin Status' is 'Tx Rx'. 'SNMP Notification' and 'MED Notification' are both 'Enabled'. Under 'Basic Optional TLVs', 'Management Address', 'Port Description', 'System Capabilities', 'System Description', and 'System Name' are unchecked. Under '802.1 Organizationally Specific TLVs', 'Protocol Identity', 'VLAN ID', 'VLAN Name', and 'Port and Protocol VLAN ID' are checked. Under '802.3 Organizationally Specific TLVs', 'Link Aggregation', 'Max Frame Size', and 'MAC/PHY Configuration/Status' are unchecked. Under 'MED TLVs', 'Capabilities', 'Extended Power', 'Inventory', 'Location', and 'Network Policy' are unchecked. The 'MED-Location Civic Address' section shows 'Country' as 'US' and 'Device entry refers to' as 'Location of the client'. A note states: 'Note: The country string shall be a two-letter ISO 3166 country code, e.g. US'. At the bottom are 'Apply' and 'Revert' buttons.

CONFIGURING LLDP INTERFACE CIVIC- ADDRESS

Use the Administration > LLDP (Configure Interface – Add CA-Type) page to specify the physical location of the device attached to an interface.

CLI REFERENCES

- ◆ ["lldp med-location civic-addr" on page 1282](#)

COMMAND USAGE

- ◆ Use the Civic Address type (CA-Type) to advertise the physical location of the device attached to an interface, including items such as the city, street number, building and room information. The address location is

specified as a type and value pair, with the civic address type defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 25: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

- ◆ Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **CA-Type** – Descriptor of the data civic address value. (Range: 0-255)
- ◆ **CA-Value** – Description of a location. (Range: 1-32 characters)

WEB INTERFACE

To specify the physical location of the attached device:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Add CA-Type from the Action list.
4. Select an interface from the Port or Trunk list.
5. Specify a CA-Type and CA-Value pair.
6. Click Apply.

Figure 232: Configuring the Civic Address for an LLDP Interface

To show the physical location of the attached device:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Show CA-Type from the Action list.
4. Select an interface from the Port or Trunk list.

Figure 233: Showing the Civic Address for an LLDP Interface

CA-Type	CA-Value
1	California

DISPLAYING LLDP LOCAL DEVICE INFORMATION

Use the Administration > LLDP (Show Local Device Information) page to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

CLI REFERENCES

- ◆ ["show lldp info local-device" on page 1289](#)

PARAMETERS

These parameters are displayed:

General Settings

- ◆ **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

Table 26: Chassis ID Subtype

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **System Name** – A string that indicates the system's administratively assigned name (see ["Displaying System Information" on page 120](#)).
- ◆ **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.
- ◆ **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

Table 27: System Capabilities

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

- ◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.
- ◆ **Management Address** – The management address associated with the local system. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- ◆ **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- ◆ **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

Interface Details

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- ◆ **Local Port/Trunk** – Local interface on this switch.
- ◆ **Port/Trunk ID Type** – There are several ways in which a port may be identified. A port ID subtype is used to indicate how the port is being referenced in the Port ID TLV.

Table 28: Port ID Subtype

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

- ◆ **Port/Trunk ID** – A string that contains the specific identifier for the local interface based on interface subtype used by this switch.
- ◆ **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- ◆ **MED Capability** – The supported set of capabilities that define the primary function(s) of the interface:
 - LLDP-MED Capabilities
 - Network Policy
 - Location Identification
 - Extended Power via MDI – PSE

- Extended Power via MDI – PD
- Inventory

WEB INTERFACE

To display LLDP information for the local device:

1. Click Administration, LLDP.
2. Select Show Local Device Information from the Step list.
3. Select General, Port, Port Details, Trunk, or Trunk Details.

Figure 234: Displaying Local Device Information for LLDP (General)

The screenshot shows the 'Administration > LLDP' configuration page. The 'Step' dropdown is set to '3. Show Local Device Information'. Under the 'General' tab, the 'LLDP Local Device Information' section displays the following details:

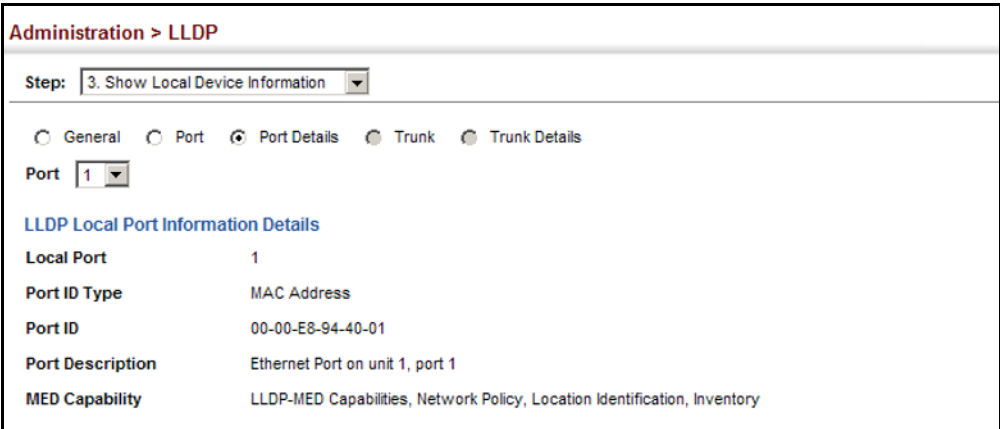
Chassis Type	MAC Address
Chassis ID	00-00-E8-94-40-00
System Name	
System Description	ECS4510-28T
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.0.3 (IPv4)

Figure 235: Displaying Local Device Information for LLDP (Port)

The screenshot shows the 'Administration > LLDP' configuration page with the 'Port' tab selected. The 'Step' dropdown is set to '3. Show Local Device Information'. The 'LLDP Local Device Port List' section shows a table with 28 total ports. The first five ports are displayed:

Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-00-E8-94-40-01
2	Ethernet Port on unit 1, port 2	00-00-E8-94-40-02
3	Ethernet Port on unit 1, port 3	00-00-E8-94-40-03
4	Ethernet Port on unit 1, port 4	00-00-E8-94-40-04
5	Ethernet Port on unit 1, port 5	00-00-E8-94-40-05

Figure 236: Displaying Local Device Information for LLDP (Port Details)



DISPLAYING LLDP
REMOTE DEVICE
INFORMATION

Use the Administration > LLDP (Show Remote Device Information) page to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

CLI REFERENCES

- ◆ ["show lldp info remote-device" on page 1290](#)

PARAMETERS

These parameters are displayed:

Port

- ◆ **Local Port** – The local port to which a remote LLDP-capable device is attached.
- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- ◆ **System Name** – A string that indicates the system's administratively assigned name.

Port Details

- ◆ **Port** – Port identifier on local switch.
- ◆ **Remote Index** – Index of remote device attached to this port.
- ◆ **Local Port** – The local port to which a remote LLDP-capable device is attached.

- ◆ **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. (See [Table 26, "Chassis ID Subtype," on page 425.](#))
- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **System Name** – A string that indicates the system's assigned name.
- ◆ **System Description** – A textual description of the network entity.
- ◆ **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field. See [Table 28, "Port ID Subtype," on page 426.](#)
- ◆ **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- ◆ **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- ◆ **System Capabilities Supported** – The capabilities that define the primary function(s) of the system. (See [Table 27, "System Capabilities," on page 425.](#))
- ◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See [Table 27, "System Capabilities," on page 425.](#))
- ◆ **Management Address List** – The management addresses for this device. 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.

If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Port Details – 802.1 Extension Information

- ◆ **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
- ◆ **Remote Port-Protocol VLAN List** – The port-based protocol VLANs configured on this interface, whether the given port (associated with the remote system) supports port-based protocol VLANs, and whether the port-based protocol VLANs are enabled on the given port associated with the remote system.
- ◆ **Remote VLAN Name List** – VLAN names associated with a port.
- ◆ **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular

protocol identity, and an octet string used to identify the protocols associated with a port of the remote system.

Port Details – 802.3 Extension Port Information

- ◆ **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.
- ◆ **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

Table 29: Remote Port Auto-Negotiation Advertised Capability

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

- ◆ **Remote Port Auto-Neg Status** – Shows whether port auto-negotiation is enabled on a port associated with the remote system.
- ◆ **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID.

Port Details – 802.3 Extension Power Information

- ◆ **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).

- ◆ **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.
- ◆ **Remote Power Pairs** – “Signal” means that the signal pairs only are in use, and “Spare” means that the spare pairs only are in use.
- ◆ **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.
- ◆ **Remote Power Pair Controllable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.
- ◆ **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements.

Port Details – 802.3 Extension Trunk Information

- ◆ **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.
- ◆ **Remote Link Aggregation Status** – The current aggregation status of the link.
- ◆ **Remote Link Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero.

Port Details – 802.3 Extension Frame Information

- ◆ **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

Port Details – LLDP-MED Capability ¹⁵

- ◆ **Device Class** – Any of the following categories of endpoint devices:
 - Class 1 – The most basic class of endpoint devices.
 - Class 2 – Endpoint devices that supports media stream capabilities.
 - Class 3 – Endpoint devices that directly supports end users of the IP communication systems.
 - Network Connectivity Device – Devices that provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. These may be any LAN access device including LAN switch/router, IEEE 802.1 bridge, IEEE 802.3 repeater, IEEE 802.11 wireless

15. These fields are only displayed for end-node devices advertising LLDP-MED TLVs.

access point, or any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

- ◆ **Supported Capabilities** – The supported set of capabilities that define the primary function(s) of the port:
 - LLDP-MED Capabilities
 - Network Policy
 - Location Identification
 - Extended Power via MDI – PSE
 - Extended Power via MDI – PD
 - Inventory
- ◆ **Current Capabilities** – The set of capabilities that define the primary function(s) of the port which are currently enabled.

Port Details – Network Policy¹⁵

- ◆ **Application Type** – The primary application(s) defined for this network policy:
 - Voice
 - Voice Signaling
 - Guest Signaling
 - Guest Voice Signaling
 - Softphone Voice
 - Video Conferencing
 - Streaming Video
 - Video Signaling
- ◆ **Tagged Flag** – Indicates whether the specified application type is using a tagged or untagged VLAN.
- ◆ **Layer 2 Priority** – The Layer 2 priority to be used for the specified application type. This field may specify one of eight priority levels (0-7), where a value of 0 represents use of the default priority.
- ◆ **Unknown Policy Flag** – Indicates that an endpoint device wants to explicitly advertise that this policy is required by the device, but is currently unknown.
- ◆ **VLAN ID** – The VLAN identifier (VID) for the port as defined in IEEE 802.1Q. A value of zero indicates that the port is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
- ◆ **DSCP Value** – The DSCP value to be used to provide Diffserv node behavior for the specified application type. This field may contain one of

64 code point values (0-63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Details – Location Identification¹⁵

- ◆ **Location Data Format** – Any of these location ID data formats:
 - Coordinate-based LCI¹⁶ – Defined in RFC 3825, includes latitude resolution, latitude, longitude resolution, longitude, altitude type, altitude resolution, altitude, and datum.
 - Civic Address LCI¹⁶ – Includes What, Country code, CA type, CA length and CA value. “What” is described as the field entry “Device entry refers to” under [“Configuring LLDP Interface Attributes.”](#) The other items are described under [“Configuring LLDP Interface Civic-Address.”](#)
 - ECS ELIN – Emergency Call Service Emergency Location Identification Number supports traditional PSAP-based Emergency Call Service in North America.
- ◆ **Country Code** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)
- ◆ **What** – The type of device to which the location applies as described for the field entry “Device entry refers to” under [“Configuring LLDP Interface Attributes.”](#)

Port Details – Extended Power-via-MDI

- ◆ **Power Type** – Power Sourcing Entity (PSE) or Power Device (PD).
- ◆ **Power Priority** – Shows power priority for a port. (Unknown, Low, High, Critical)
- ◆ **Power Source** – Shows information based on the type of device:
 - **PD** – Unknown, PSE, Local, PSE and Local
 - **PSE** – Unknown, Primary Power Source, Backup Power Source - Power conservation mode
- ◆ **Power Value** – The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. This parameter supports a maximum power required or available value of 102.3 Watts to allow for future expansion. (Range: 0 - 102.3 Watts)

Port Details – Inventory¹⁵

- ◆ **Hardware Revision** – The hardware revision of the end-point device.
- ◆ **Software Revision** – The software revision of the end-point device.

¹⁶. Location Configuration Information

- ◆ **Manufacture Name** – The manufacturer of the end-point device
- ◆ **Asset ID** – The asset identifier of the end-point device. End-point devices are typically assigned asset identifiers to facilitate inventory management and assets tracking.
- ◆ **Firmware Revision** – The firmware revision of the end-point device.
- ◆ **Serial Number** – The serial number of the end-point device.
- ◆ **Model Name** – The model name of the end-point device.

WEB INTERFACE

To display LLDP information for a remote port:

1. Click Administration, LLDP.
2. Select Show Remote Device Information from the Step list.
3. Select Port, Port Details, Trunk, or Trunk Details.
4. When the next page opens, select a port on this switch and the index for a remote device attached to this port.
5. Click Query.

Figure 237: Displaying Remote Device Information for LLDP (Port)

The figure consists of two screenshots of a web interface for displaying LLDP information.

Top Screenshot: The interface shows the breadcrumb "Administration > LLDP" and a "Step:" dropdown set to "4. Show Remote Device Information". Below this are radio buttons for "Port" (selected), "Port Details", "Trunk", and "Trunk Details". A section titled "LLDP Remote Device Port List" shows "Total: 1". Below is a table:

Local Port	Chassis ID	Port ID	System Name
1	70-72-CF-32-DD-FD	70-72-CF-32-DD-FF	RD93

Bottom Screenshot: The interface shows the same breadcrumb and "Step:" dropdown. The radio buttons are now "Port", "Port Details" (selected), "Trunk", and "Trunk Details". Below are two dropdown menus: "Port" with value "1" and "Remote Index" with value "2". A "Query" button is at the bottom right.

Figure 238: Displaying Remote Device Information for LLDP (Port Details)

Administration > LLDP

Step: 4. Show Remote Device Information

☐ Port
☒ Port Details
☐ Trunk
☐ Trunk Details

Port: 23

Remote Index: 4

Query

LLDP Remote Device Port Information

Local Port	23	Port Type	MAC Address
Chassis Type	MAC Address	Port Description	Ethernet Port on unit 1, port 1
Chassis ID	00-E0-00-00-00-01	Port ID	00-E0-00-00-00-02
System Name		System Capabilities Supported	Bridge
System Description	ES3528MV2	System Capabilities Enabled	Bridge

Management Address List Total: 1

Address	Address Type
192.168.0.3	IPv4 Address

802.1 Extension Information

Remote Port VID: 1

Remote Port-Protocol VLAN List Total: 1

VLAN	Support	Status
1	Yes	Enabled

Remote VLAN Name List Total: 1

VLAN	Name
1	DefaultVlan

Remote Protocol Identity List Total: 1

Remote Protocol Identity (Hex)
88-CC

802.3 Extension Port Information

Remote Port Auto-Neg Supported	Yes	Remote Port Auto-Neg Status	Enabled
Remote Port Auto-Neg Adv-Capability	0000	Remote Port MAU Type	6

802.3 Extension Power Information

Remote Power Class	PSE	Remote Power MDI Supported	Yes
Remote Power MDI Status	Enabled	Remote Power Pair Controlable	No
Remote Power Pairs	Spare	Remote Power Classification	Class1

802.3 Extension Trunk Information

Remote Link Aggregation Capable	Yes	Remote Link Aggregation Status	Disabled
Remote Link Port ID	0		

802.3 Extension Frame Information

Remote Max Frame Size	1518
-----------------------	------

Additional information displayed by an end-point device which advertises LLDP-MED TLVs is shown in the following figure.

Figure 239: Displaying Remote Device Information for LLDP (End Node)

Administration > LLDP

Step: 4. Show Remote Device Information

LLDP-MED Capability

Device Class

Network Connectivity

Supported Capabilities

LLDP-MED Capabilities, Network Policy, Location Identification, Inventory

Current Capabilities

LLDP-MED Capabilities, Network Policy, Location Identification, Inventory

Network Policy

Application Type

Guest Voice Signaling

Unknown Policy Flag

Disabled

Tagged Flag

Disabled

VLAN ID

7

Layer 2 Priority

2

DSCP Value

62

Location Identification

Location Data Format

Coordinate-based LCI

Country Code

TW

What

2

Location Identification

Location Data Format

Civic Address LCI

Country Code

US

What

2

Extended Power-via-MDI

Power Type

PSE

Power Source

Unknown

Power Priority

Unknown

Power Value

0 W Watts

Inventory

Hardware Revision

R01

Firmware Revision

1.2.2.1

Software Revision

1.2.2.1

Serial Number

LN10230092

Manufacture Name

Model Name

L

Asset ID

DISPLAYING DEVICE STATISTICS

Use the Administration > LLDP (Show Device Statistics) page to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

CLI REFERENCES

- ◆ ["show lldp info statistics" on page 1293](#)

PARAMETERS

These parameters are displayed:

General Statistics on Remote Devices

- ◆ **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- ◆ **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- ◆ **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

- ◆ **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
- ◆ **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Port/Trunk

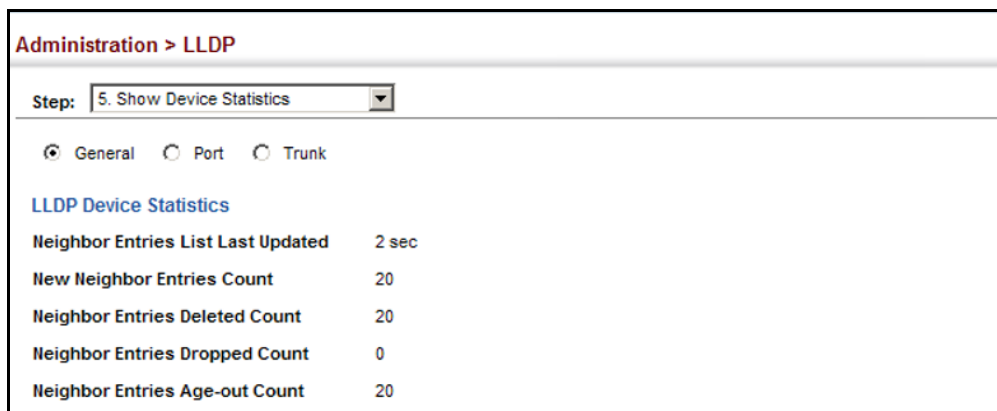
- ◆ **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
- ◆ **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.
- ◆ **Frames Received** – Number of LLDP PDUs received.
- ◆ **Frames Sent** – Number of LLDP PDUs transmitted.
- ◆ **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- ◆ **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- ◆ **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

WEB INTERFACE

To display statistics for LLDP-capable devices attached to the switch:

1. Click Administration, LLDP.
2. Select Show Device Statistics from the Step list.
3. Select General, Port, or Trunk.

Figure 240: Displaying LLDP Device Statistics (General)



Administration > LLDP

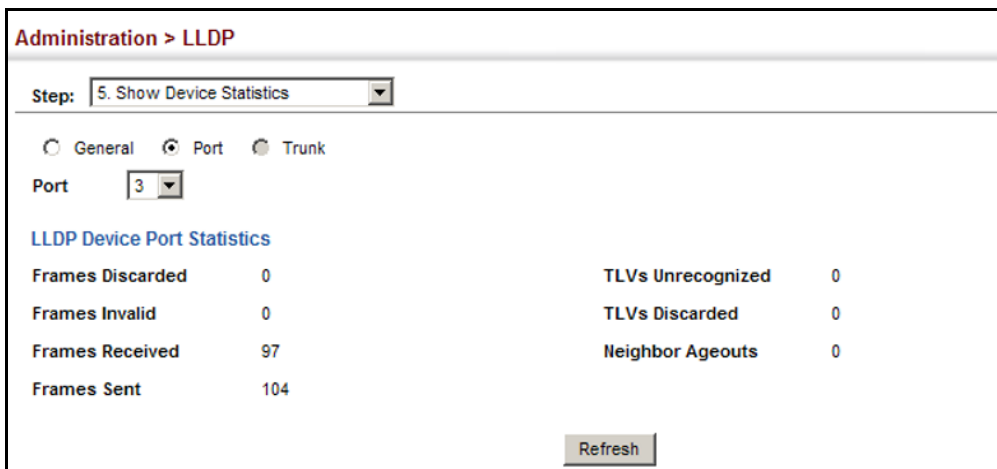
Step: 5. Show Device Statistics

☒ General ☐ Port ☐ Trunk

LLDP Device Statistics

Neighbor Entries List Last Updated	2 sec
New Neighbor Entries Count	20
Neighbor Entries Deleted Count	20
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	20

Figure 241: Displaying LLDP Device Statistics (Port)



Administration > LLDP

Step: 5. Show Device Statistics

☐ General ☒ Port ☐ Trunk

Port 3

LLDP Device Port Statistics

Frames Discarded	0	TLVs Unrecognized	0
Frames Invalid	0	TLVs Discarded	0
Frames Received	97	Neighbor Ageouts	0
Frames Sent	104		

Refresh

POWER OVER ETHERNET

The ECS4510-28P/52P can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-compliant devices (IEEE 802.3af or 802.3at).

The switch's power management enables individual port power to be controlled within the switch's power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Ports can be set to one of three power priority levels, critical, high, or low. To control the power supply within the switch's budget, ports set at critical to high priority have power enabled in preference to those ports set at low priority. For example, when a device connected to a port is set to critical priority, the switch supplies the required power, if necessary by denying power to ports set for a lower priority during bootstrap.



NOTE: For more information on using the PoE provided by this switch refer to the Installation Guide.

DISPLAYING THE SWITCH'S OVERALL PoE POWER BUDGET

Use the Administration > PoE (Configure Global) page to display the maximum PoE power budget for the switch (power available to all RJ-45 ports). The maximum power budget is fixed at the maximum available setting, which prevents overload conditions at the power source. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

CLI REFERENCES

- ◆ ["Power over Ethernet Commands" on page 1007](#)

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **PoE Maximum Available Power** – The power budget for the switch. If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power. (Fixed: ECS4510-28P/52P - 410/780 Watts)
- ◆ **System Operation Status** – Status of the PoE power service provided to the switch ports.
- ◆ **PoE Power Consumption** – The amount of power being consumed by PoE devices connected to the switch.
- ◆ **Software Version** – The version of software running on the PoE controller subsystem in the switch.

WEB INTERFACE

To set the overall PoE power budget for switch in the web interface:

1. Click Administration, PoE.
2. Select Configure Global from the Step list.

Figure 242: Showing the Switch's PoE Budget (ECS4510-28P)

The screenshot shows a web-based configuration interface for a switch. At the top, there is a breadcrumb trail 'Administration > PoE'. Below this is a 'Step:' dropdown menu currently set to '1. Configure Global'. The main content area is titled 'Mainpower Status' and contains a table with the following information:

PoE Maximum Available Power	410 Watts
System Operation Status	On
PoE Power Consumption	0 Watts
Software Version	Version 0x0148, Build 0x66

SETTING THE PORT PoE POWER BUDGET Use the Administration > PoE (Configure Interface) page to set the maximum power provided to a port.

CLI REFERENCES

- ◆ ["Power over Ethernet Commands" on page 1007](#)
- ◆ ["Time Range" on page 776](#)

COMMAND USAGE

- ◆ This switch supports both the IEEE 802.3af PoE and IEEE 802.3at-2009 PoE Plus standards. To ensure that the correct power is supplied to powered devices (PD) compliant with these standards, the first detection pulse from the switch is based on 802.3af to which the 802.3af PDs will respond normally. It then sends a second PoE Plus pulse that causes an 802.3at PD to respond as a Class 4 device and draw Class 4 current. Afterwards, the switch exchanges information with the PD such as duty-cycle, peak and average power needs.
- ◆ All the RJ-45 ports support both the IEEE 802.3af and IEEE 802.3at standards.
 - For the ECS4510-28P, the total PoE power delivered by all ports cannot exceed the maximum power budget of 410W. This means that up to 13 ports can supply a maximum 30W of power simultaneously to connected devices (802.3at), or up to 24 ports can supply up to 15.4W (802.3af).
 - For the ECS4510-52P, the total PoE power delivered by all ports cannot exceed the maximum power budget of 780W. This means that up to 25 ports can supply a maximum 30W of power simultaneously to connected devices (802.3at), or up to 48 ports can supply up to 15.4W (802.3af).
- ◆ If a device is connected to a switch port and the switch detects that it requires more than the power budget set for the port or to the overall switch, no power is supplied to the device (i.e., port power remains off).

- ◆ If the power demand from devices connected to all switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:
 - If a device is connected to a low-priority port and causes the switch to exceed its budget, power to this port is not turned on.
 - If a device is connected to a critical or high-priority port and would cause the switch to exceed its power budget as determined during bootup, power is provided to the port only if the switch can drop power to one or more lower-priority ports and thereby remain within its overall budget.
 - If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port regardless of its priority setting.
 - If priority is not set for any ports, and there is not sufficient power to supply all of the ports, port priority defaults to Port 1, Port 2, Port 3 ... Port 24¹⁷/48¹⁸, with available power being supplied in that sequence.
 - If priority is not set for any ports, and PoE consumption exceeds the maximum power provided by the switch, power is shut down in the reverse sequence, starting from Port 24/48.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Port** – The port number on the switch.
- ◆ **Admin Status** – Enables PoE power on a port. Power is automatically supplied when a device is detected on a port, providing that the power demanded does not exceed the switch or port power budget. (Default: Enabled)
- ◆ **Mode** – Shows whether or not PoE power is being supplied to a port.
- ◆ **Priority** – Sets the power priority for a port. (Options: Low, High, or Critical; Default: Low)
- ◆ **Power Allocation** – Sets the power budget for a port. (Range: 3000-30000 milliwatts; Default: 30000 milliwatts)
- ◆ **Power Consumption** – Current power consumption on a port.

17. ECS4510-28P

18. ECS4510-52P

WEB INTERFACE

To set the PoE power budget for a port:

1. Click Administration, PoE.
2. Select Configure Interface from the Step list.
3. Enable PoE power on selected ports. Set the priority and the power allocation.
4. Click Apply.

Figure 243: Setting a Port's PoE Budget

The screenshot shows a web interface titled "Administration > PoE". Below the title is a "Step:" dropdown menu set to "2. Configure Interface". The main section is titled "PoE Port List Total: 24" and contains a table with 10 rows. Each row represents a port with columns for Port, Admin Status, Mode, Priority, Power Allocation, and Power Consumption (milliwatts). All ports are currently "Enabled", "Off", "Low", and have a "Power Allocation" of 30000 (except for port 1 which is 99999) and "Power Consumption" of 0. At the bottom right of the table are "Apply" and "Revert" buttons.

Port	Admin Status	Mode	Priority	Power Allocation	Power Consumption (milliwatts)
1	<input checked="" type="checkbox"/> Enabled	Off	Low	99999	0
2	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
3	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
4	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
5	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
6	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
7	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
8	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
9	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0
10	<input checked="" type="checkbox"/> Enabled	Off	Low	30000	0

SIMPLE NETWORK MANAGEMENT PROTOCOL

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware,

as well as the traffic passing through its ports. A network management station can access this information using network management software. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having its own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to “groups” that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as “views.” The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 30: SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	Community string only
v3	noAuthNoPriv	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	A user name match only
v3	AuthNoPriv	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	<i>user defined</i>	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption



NOTE: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

COMMAND USAGE

Configuring SNMPv1/2c Management Access

To configure SNMPv1 or v2c management access to the switch, follow these steps:

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.
2. Use the Administration > SNMP (Configure User - Add Community) page to configure the community strings authorized for management access.
3. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

Configuring SNMPv3 Management Access

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.
2. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.
3. Use the Administration > SNMP (Configure Engine) page to change the local engine ID. If you want to change the default engine ID, it must be changed before configuring other parameters.
4. Use the Administration > SNMP (Configure View) page to specify read and write access views for the switch MIB tree.
5. Use the Administration > SNMP (Configure User) page to configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).
6. Use the Administration > SNMP (Configure Group) page to assign SNMP users to groups, along with their specific authentication and privacy passwords.

CONFIGURING GLOBAL SETTINGS FOR SNMP

Use the Administration > SNMP (Configure Global) page to enable SNMPv3 service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.

CLI REFERENCES

- ◆ ["snmp-server" on page 787](#)
- ◆ ["snmp-server enable traps" on page 790](#)

PARAMETERS

These parameters are displayed:

- ◆ **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- ◆ **Authentication Traps**¹⁹ – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)
- ◆ **Link-up and Link-down Traps**¹⁹ – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

WEB INTERFACE

To configure global settings for SNMP:

1. Click Administration, SNMP.
2. Select Configure Global from the Step list.
3. Enable SNMP and the required trap types.
4. Click Apply

Figure 244: Configuring Global Settings for SNMP

The screenshot shows a web interface for configuring SNMP. The breadcrumb is 'Administration > SNMP'. Below it is a 'Step:' dropdown menu set to '1. Configure Global'. The main content area contains three settings, each with a checked checkbox and the word 'Enabled': 'Agent Status', 'Authentication Traps', and 'Link-up and Link-down Traps'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

SETTING THE LOCAL ENGINE ID

Use the Administration > SNMP (Configure Engine - Set Engine ID) page to change the local engine ID. An SNMPv3 engine is an independent SNMP agent that resides on the switch. 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.

CLI REFERENCES

- ◆ ["snmp-server engine-id" on page 793](#)

COMMAND USAGE

- ◆ 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

19. These are legacy notifications and therefore when used for SNMPv3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View ([page 448](#)).

ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

PARAMETERS

These parameters are displayed:

- ◆ **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".
- ◆ **Engine Boots** – The number of times that the engine has (re-)initialized since the SNMP EngineID was last configured.

WEB INTERFACE

To configure the local SNMP engine ID:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Set Engine ID from the Action list.
4. Enter an ID of a least 9 hexadecimal characters.
5. Click Apply

Figure 245: Configuring the Local Engine ID for SNMP

Administration > SNMP

Step: 2. Configure Engine Action: Set Engine ID

Engine ID 800001030300000c0000fd0000

Engine Boots 5

Default Save

SPECIFYING A REMOTE ENGINE ID

Use the Administration > SNMP (Configure Engine - Add Remote Engine) page to configure a engine ID for a remote management station. To allow management access from an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. 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.

CLI REFERENCES

- ◆ ["snmp-server engine-id" on page 793](#)

COMMAND USAGE

- ◆ 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. (See ["Configuring Remote SNMPv3 Users" on page 459.](#))

PARAMETERS

These parameters are displayed:

- ◆ **Remote Engine ID** – The engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".
- ◆ **Remote IP Host** – The IP address of a remote management station which is using the specified engine ID.

WEB INTERFACE

To configure a remote SNMP engine ID:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Add Remote Engine from the Action list.
4. Enter an ID of a least 9 hexadecimal characters, and the IP address of the remote host.
5. Click Apply

Figure 246: Configuring a Remote Engine ID for SNMP

The screenshot shows a web interface titled "Administration > SNMP". It features two dropdown menus: "Step:" set to "2. Configure Engine" and "Action:" set to "Add Remote Engine". Below these are two text input fields: "Remote Engine ID" containing "5432100000" and "Remote IP Host" containing "192.168.1.19". At the bottom right are "Apply" and "Revert" buttons.

To show the remote SNMP engine IDs:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Show Remote Engine from the Action list.

Figure 247: Showing Remote Engine IDs for SNMP

The screenshot shows the 'Administration > SNMP' configuration page. At the top, there is a breadcrumb trail 'Administration > SNMP'. Below it, there are two dropdown menus: 'Step: 2. Configure Engine' and 'Action: Show Remote Engine'. The main content area is titled 'SNMPv3 Remote Engine List' with a 'Total: 1' indicator. It contains a table with two columns: 'Remote Engine ID' and 'Remote IP Host'. The table has one row with the values '5432100000' and '192.168.1.19'. Below the table, there are 'Delete' and 'Revert' buttons.

Remote Engine ID	Remote IP Host
5432100000	192.168.1.19

SETTING SNMPv3 VIEWS

Use the Administration > SNMP (Configure View) page to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

CLI REFERENCES

- ◆ ["snmp-server view" on page 797](#)

PARAMETERS

These parameters are displayed:

Add View

- ◆ **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- ◆ **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers. (Range: 1-64 characters)
- ◆ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Add OID Subtree

- ◆ **View Name** – Lists the SNMP views configured in the Add View page. (Range: 1-64 characters)
- ◆ **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string. (Range: 1-64 characters)
- ◆ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

WEB INTERFACE

To configure an SNMP view of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.

3. Select Add View from the Action list.
4. Enter a view name and specify the initial OID subtree in the switch's MIB database to be included or excluded in the view. Use the Add OID Subtree page to add additional object identifier branches to the view.
5. Click Apply

Figure 248: Creating an SNMP View

Administration > SNMP

Step: 3. Configure View Action: Add View

View Name: ifEntry.a

OID Subtree: 1.3.6.1.2.1.2.2.1.1.*

Type: Included

Apply Revert

To show the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show View from the Action list.

Figure 249: Showing SNMP Views

Administration > SNMP

Step: 3. Configure View Action: Show View

SNMPv3 View List Total: 2

	View Name
<input type="checkbox"/>	ifEntry.a
<input type="checkbox"/>	defaultview

Delete Revert

To add an object identifier to an existing SNMP view of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Add OID Subtree from the Action list.
4. Select a view name from the list of existing views, and specify an additional OID subtree in the switch's MIB database to be included or excluded in the view.

5. Click Apply

Figure 250: Adding an OID Subtree to an SNMP View

Administration > SNMP

Step: 3. Configure View Action: Add OID Subtree

View Name ifEntry.a

OID Subtree 1.3.6.1.2.1.2.2.1.2.*

Type Included

Apply Revert

To show the OID branches configured for the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show OID Subtree from the Action list.
4. Select a view name from the list of existing views.

Figure 251: Showing the OID Subtree Configured for SNMP Views

Administration > SNMP

Step: 3. Configure View Action: Show OID Subtree

View Name ifEntry.a

SNMPv3 View OID Subtree List Total: 2

<input type="checkbox"/>	OID Subtree	Type
<input type="checkbox"/>	1.3.6.1.2.1.2.2.1.1.*	Included
<input type="checkbox"/>	1.3.6.1.2.1.2.2.1.2.*	Included

Delete Revert

CONFIGURING SNMPv3 GROUPS

Use the Administration > SNMP (Configure Group) page to add an SNMPv3 group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

CLI REFERENCES

- ◆ ["show snmp group" on page 798](#)

PARAMETERS

These parameters are displayed:

- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3.
- ◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- ◆ **Read View** – The configured view for read access. (Range: 1-32 characters)
- ◆ **Write View** – The configured view for write access. (Range: 1-32 characters)
- ◆ **Notify View** – The configured view for notifications. (Range: 1-32 characters)

Table 31: Supported Notification Messages

Model	Level	Group
<i>RFC 1493 Traps</i>		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
<i>SNMPv2 Traps</i>		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
<i>RMON Events (V2)</i>		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.
<i>Private Traps</i>		
swPowerStatusChangeTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.1	This trap is sent when the power state changes.
swPortSecurityTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.

Table 31: Supported Notification Messages (Continued)

Model	Level	Group
swIpFilterRejectTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swAuthenticationFailure	1.3.6.1.4.1.259.10.1.24.1.2.1.0.66	This trap will be triggered if authentication fails.
swAuthenticationSuccess	1.3.6.1.4.1.259.10.1.24.1.2.1.0.67	This trap will be triggered if authentication is successful.
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.70	When broadcast traffic is detected as a storm, this trap is fired.
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.71	When a broadcast storm is detected as normal traffic, this trap is fired.
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.72	When ATC is activated, this trap is fired.
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.73	When ATC is released, this trap is fired.
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.74	When multicast traffic is detected as the storm, this trap is fired.
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.75	When multicast storm is detected as normal traffic, this trap is fired.
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.76	When ATC is activated, this trap is fired.
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.77	When ATC is released, this trap is fired.
swLoopbackDetectionTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.95	This trap is sent when loopback BPDUs have been detected.
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.96	This trap is sent when a networkAccessPortLinkDetection event is triggered.
dot1agCfmMepUpTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.97	This trap is sent when a new remote MEP is discovered.
dot1agCfmMepDownTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.98	This trap is sent when port status or interface status TLV received from remote MEP indicates it is not up.
dot1agCfmConfigFailTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.99	This trap is sent when a MEP receives a CCM with MPID which already exists on the same MA in this switch.
dot1agCfmLoopFindTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.100	This trap is sent when a MEP receives its own CCMs.
dot1agCfmMepUnknownTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.101	This trap is sent when a CCM is received from an unexpected MEP.
dot1agCfmMepMissingTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.102	This trap is sent when the cross-check enable timer expires and no CCMs were received from an expected (configured) MEP.
dot1agCfmMaUpTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.103	This trap is sent when all expected remote MEPs are up.
autoUpgradeTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.104	This trap is sent when auto upgrade is executed.
swCpuUtiRisingNotification	1.3.6.1.4.1.259.10.1.24.1.2.1.0.107	This notification indicates that the CPU utilization has risen from cpuUtiFallingThreshold to cpuUtiRisingThreshold.
swCpuUtiFallingNotification	1.3.6.1.4.1.259.10.1.24.1.2.1.0.108	This notification indicates that the CPU utilization has fallen from cpuUtiRisingThreshold to cpuUtiFallingThreshold.

Table 31: Supported Notification Messages (Continued)

Model	Level	Group
swMemoryUtiRisingThreshold Notification	1.3.6.1.4.1.259.10.1.24.1.2.1.0.109	This notification indicates that the memory utilization has risen from memoryUtiFallingThreshold to memoryUtiRisingThreshold.
swMemoryUtiFallingThreshold Notification	1.3.6.1.4.1.259.10.1.24.1.2.1.0.110	This notification indicates that the memory utilization has fallen from memoryUtiRisingThreshold to memoryUtiFallingThreshold.
dhcpRogueServerAttackTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.114	This trap is sent when receiving a DHCP packet from a rouge server.
swLoginFailureTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.139	This trap is sent when login fails via console, telnet or web.
swLoginSucceedTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.140	This trap is sent when login succeeds via console, telnet or web.
lbdDetectionTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.141	This trap is sent when a loopback condition is detected by LBD.
lbdRecoveryTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.142	This trap is sent when a recovery is done by LBD.
udldPortShutdownTrap	1.3.6.1.4.1.259.10.1.24.1.2.1.0.192	This trap is sent when the port is shut down by UDLD.

* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

WEB INTERFACE

To configure an SNMP group:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Enter a group name, assign a security model and level, and then select read, write, and notify views.
5. Click Apply

Figure 252: Creating an SNMP Group

Administration > SNMP

Step: 4. Configure Group Action: Add

Group Name:

Security Model:

Security Level:

Read View: ☒ ☐

Write View: ☒ ☐

Notify View: ☒ ☐

To show SNMP groups:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 253: Showing SNMP Groups

Administration > SNMP

Step: 4. Configure Group Action: Show

SNMPv3 Group List Total: 5

<input type="checkbox"/>	Group Name	Model	Level	Read View	Write View	Notify View
<input type="checkbox"/>	public	v1	noAuthNoPriv	defaultview	none	none
<input type="checkbox"/>	public	v2c	noAuthNoPriv	defaultview	none	none
<input type="checkbox"/>	private	v1	noAuthNoPriv	defaultview	defaultview	none
<input type="checkbox"/>	private	v2c	noAuthNoPriv	defaultview	defaultview	none
<input type="checkbox"/>	secure-users	v3	authPriv	ifEntry.a	ifEntry.a	ifEntry.a

SETTING COMMUNITY ACCESS STRINGS Use the Administration > SNMP (Configure User - Add Community) page to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

CLI REFERENCES

- ◆ ["snmp-server community" on page 787](#)

PARAMETERS

These parameters are displayed:

- ◆ **Community String** – A community string that acts like a password and permits access to the SNMP protocol.
Range: 1-32 characters, case sensitive
Default strings: "public" (Read-Only), "private" (Read/Write)
- ◆ **Access Mode** – Specifies the access rights for the community string:
 - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
 - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

WEB INTERFACE

To set a community access string:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add Community from the Action list.
4. Add new community strings as required, and select the corresponding access rights from the Access Mode list.
5. Click Apply

Figure 254: Setting Community Access Strings

Administration > SNMP

Step: 5. Configure User Action: Add Community

Community String spiderman

Access Mode Read/Write

Apply Revert

To show the community access strings:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show Community from the Action list.

Figure 255: Showing Community Access Strings

Administration > SNMP

Step: 5. Configure User Action: Show Community

SNMP Community String List Total: 3

	Community String	Access Mode
<input type="checkbox"/>	public	Read-Only
<input type="checkbox"/>	private	Read/Write
<input type="checkbox"/>	spiderman	Read/Write

Delete Revert

CONFIGURING LOCAL SNMPV3 USERS

Use the Administration > SNMP (Configure User - Add SNMPv3 Local User) page to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

CLI REFERENCES

- ◆ ["snmp-server user" on page 795](#)

PARAMETERS

These parameters are displayed:

- ◆ **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3.
- ◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.

- **AuthPriv** – SNMP communications use both authentication and encryption.
- ◆ **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- ◆ **Authentication Password** – A minimum of eight plain text characters is required.
- ◆ **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- ◆ **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a local SNMPv3 user:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add SNMPv3 Local User from the Action list.
4. Enter a name and assign it to a group. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
5. Click Apply

Figure 256: Configuring Local SNMPv3 Users

The screenshot shows a web interface for configuring a local SNMPv3 user. The breadcrumb path is "Administration > SNMP". The "Step" dropdown is set to "5. Configure User" and the "Action" dropdown is set to "Add SNMPv3 Local User".

SNMPv3 User

User Name:

Group Name: ☐ public ☒ r&d

Security Model:

Security Level:

User Authentication

Authentication Protocol:

Authentication Password:

Data Privacy

Privacy Protocol:

Privacy Password:

Buttons:

To show local SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Local User from the Action list.

Figure 257: Showing Local SNMPv3 Users

Administration > SNMP						
Step: 5. Configure User Action: Show SNMPv3 Local User						
SNMPv3 Local User List Total: 1						
<input type="checkbox"/>	User Name	Group Name	Model	Level	Authentication	Privacy
<input type="checkbox"/>	chris	r&d	v3	authPriv	MD5	DES56
Delete Revert						

CONFIGURING REMOTE SNMPv3 USERS

Use the Administration > SNMP (Configure User - Add SNMPv3 Remote User) page to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

CLI REFERENCES

- ◆ ["snmp-server user" on page 795](#)

COMMAND USAGE

- ◆ To grant management access to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and the remote user. (See ["Specifying Trap Managers" on page 462](#) and ["Specifying a Remote Engine ID" on page 446](#).)

PARAMETERS

These parameters are displayed:

- ◆ **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Remote IP** – The Internet address of the remote device where the user resides.
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)

- ◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- ◆ **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- ◆ **Authentication Password** – A minimum of eight plain text characters is required.
- ◆ **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- ◆ **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a remote SNMPv3 user:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add SNMPv3 Remote User from the Action list.
4. Enter a name and assign it to a group. Enter the IP address to identify the source of SNMPv3 inform messages sent from the local switch. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
5. Click Apply

Figure 258: Configuring Remote SNMPv3 Users

Administration > SNMP

Step: 5. Configure User Action: Add SNMPv3 Remote User

SNMPv3 User

User Name: mark

Group Name: ☐ public ☒ r&d

Remote IP: 192.168.1.19

Security Model: v3

Security Level: authPriv

User Authentication

Authentication Protocol: MD5

Authentication Password: greenpeace

Data Privacy

Privacy Protocol: DES56

Privacy Password: einstien

Apply Revert

To show remote SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Remote User from the Action list.

Figure 259: Showing Remote SNMPv3 Users

Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Remote User

SNMPv3 Remote User List Total: 1

<input type="checkbox"/>	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
<input type="checkbox"/>	mark	r&d	5432100000	v3	authPriv	MD5	DES56

Delete Revert

SPECIFYING TRAP MANAGERS

Use the Administration > SNMP (Configure Trap) page to specify the host devices to be sent traps and the types of traps to send. Traps indicating status changes are issued by the switch to the specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

CLI REFERENCES

- ◆ "snmp-server host" on page 791
- ◆ "snmp-server enable traps" on page 790

COMMAND USAGE

- ◆ 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 444](#)).
2. Create a view with the required notification messages ([page 448](#)).
3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view ([page 451](#)).
4. Enable trap informs as described in the following pages.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent ([page 444](#)).
2. Create a local SNMPv3 user to use in the message exchange process ([page 457](#)). If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified local user, and default settings for the read, write, and notify view.
3. Create a view with the required notification messages ([page 448](#)).
4. Create a group that includes the required notify view ([page 451](#)).
5. Enable trap informs as described in the following pages.

PARAMETERS

These parameters are displayed:

SNMP Version 1

- ◆ **IP Address** – IPv4 or IPv6 address of a new management station to receive notification message (i.e., the targeted recipient).
- ◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- ◆ **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.

- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 2c

- ◆ **IP Address** – IPv4 or IPv6 address of a new management station to receive notification message (i.e., the targeted recipient).
- ◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- ◆ **Notification Type**

- **Traps** – Notifications are sent as trap messages.
- **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
 - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

- ◆ **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.

- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 3

- ◆ **IP Address** – IPv4 or IPv6 address of a new management station to receive notification message (i.e., the targeted recipient).
- ◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- ◆ **Notification Type**
 - **Traps** – Notifications are sent as trap messages.
 - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
 - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- ◆ **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch. (Range: 1-32 characters)

If an account for the specified user has not been created ([page 457](#)), one will be automatically generated.
- ◆ **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters)

If an account for the specified user has not been created ([page 459](#)), one will be automatically generated.
- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)
- ◆ **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.

WEB INTERFACE

To configure trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Add from the Action list.
4. Fill in the required parameters based on the selected SNMP version.
5. Click Apply

Figure 260: Configuring Trap Managers (SNMPv1)

The screenshot shows the 'Administration > SNMP' configuration page. At the top, there are two dropdown menus: 'Step: 6. Configure Trap' and 'Action: Add'. Below these, there are four input fields: 'IP Address' with the value '192.168.0.3', 'Version' with a dropdown set to 'v1', 'Community String' with the value 'private', and 'UDP Port (1-65535)' with the value '162'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

Figure 261: Configuring Trap Managers (SNMPv2c)

The screenshot shows the 'Administration > SNMP' configuration page for SNMPv2c. At the top, there are two dropdown menus: 'Step: 6. Configure Trap' and 'Action: Add'. Below these, there are seven input fields: 'IP Address' with the value '192.168.2.9', 'Version' with a dropdown set to 'v2c', 'Notification Type' with a dropdown set to 'Inform', 'Timeout (0-2147483647)' with an empty field and the unit 'centiseconds' to its right, 'Retry Times (0-255)' with an empty field, 'Community String' with the value 'venus', and 'UDP Port (1-65535)' with an empty field. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

Figure 262: Configuring Trap Managers (SNMPv3)

Administration > SNMP

Step: 6. Configure Trap Action: Add

IP Address: 192.168.2.9

Version: v3

Notification Type: Inform

Timeout (0-2147483647): centiseconds

Retry Times (0-255):

Remote User Name:

UDP Port (1-65535):

Security Level: authPriv

Apply Revert

To show configured trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Show from the Action list.

Figure 263: Showing Trap Managers

Administration > SNMP

Step: 6. Configure Trap Action: Show

SNMP Trap Manager List Total: 5

	IP Address	Version	Community String/User Name	UDP Port	Security Level	Timeout	Retry Times
<input type="checkbox"/>	192.168.0.4	v3	steve	162	noAuthNoPriv		
<input type="checkbox"/>	192.168.0.5	v3	bobby	162	noAuthNoPriv		
<input type="checkbox"/>	192.168.0.6	v3	betty	162	authNoPriv		
<input type="checkbox"/>	192.168.2.9	v2c	venus	162		1600	5
<input type="checkbox"/>	192.168.5.8	v3	margaret	162	authPriv	1600	5

Delete Revert

CREATING SNMP
NOTIFICATION LOGS

Use the Administration > SNMP (Configure Notify Filter - Add) page to create an SNMP notification log.

CLI REFERENCES

- ◆ "nlm" on page 801
- ◆ "snmp-server notify-filter" on page 801
- ◆ "show nlm oper-status" on page 803
- ◆ "show snmp notify-filter" on page 803

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 be exceeding 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, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.
- ◆ To avoid this problem, notification logging should be configured as described in this section, and these commands stored in the startup configuration file using the System > File (Copy – Running-Config) page as described on [page 127](#). Then when the switch reboots, SNMP traps (such as warm start) can now be logged.
- ◆ 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 using the Administration > SNMP (Configure Trap – Add) page described on [page 462](#), a default notify filter will be created.

PARAMETERS

These parameters are displayed:

- ◆ **IP Address** – The Internet address of a remote device. The specified target host must already have been configured using the Administration > SNMP (Configure Trap – Add) page.

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.

- ◆ **Filter Profile Name** – Notification log profile name. (Range: 1-32 characters)

WEB INTERFACE

To create an SNMP notification log:

1. Click Administration, SNMP.
2. Select Configure Notify Filter from the Step list.
3. Select Add from the Action list.
4. Fill in the IP address of a configured trap manager and the filter profile name.

5. Click Apply

Figure 264: Creating SNMP Notification Logs

Administration > SNMP

Step: 7. Configure Notify Filter Action: Add

IP Address 192.168.0.99

Filter Profile Name R&D

Apply Revert

To show configured SNMP notification logs:

1. Click Administration, SNMP.
2. Select Configure Notify Filter from the Step list.
3. Select Show from the Action list.

Figure 265: Showing SNMP Notification Logs

Administration > SNMP

Step: 7. Configure Notify Filter Action: Show

SNMP Notify Filter List Total: 1

	Filter profile name	IP Address
<input type="checkbox"/>	R&D	192.168.0.99

Delete Revert

SHOWING SNMP STATISTICS Use the Administration > SNMP (Show Statistics) page to show counters for SNMP input and output protocol data units.

CLI REFERENCES

- ◆ "show snmp" on page 789

PARAMETERS

The following counters are displayed:

- ◆ **SNMP packets input** – The total number of messages delivered to the SNMP entity from the transport service.
- ◆ **Bad SNMP version errors** – The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
- ◆ **Unknown community name** – The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.

- ◆ **Illegal operation for community name supplied** – The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
- ◆ **Encoding errors** – The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
- ◆ **Number of requested variables** – The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
- ◆ **Number of altered variables** – The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
- ◆ **Get-request PDUs** – The total number of SNMP Get-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **Get-next PDUs** – The total number of SNMP Get-Next PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **Set-request PDUs** – The total number of SNMP Set-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **SNMP packets output** – The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
- ◆ **Too big errors** – The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is "tooBig."
- ◆ **No such name errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "noSuchName."
- ◆ **Bad values errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "badValue."
- ◆ **General errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "genErr."
- ◆ **Response PDUs** – The total number of SNMP Get-Response PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.
- ◆ **Trap PDUs** – The total number of SNMP Trap PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.

WEB INTERFACE

To show SNMP statistics:

1. Click Administration, SNMP.
2. Select Show Statistics from the Step list.

Figure 266: Showing SNMP Statistics

Administration > SNMP

Step: 8. Show Statistics

SNMP Statistics

SNMP packets Input	0	SNMP packets Output	0
Bad SNMP version errors	0	Too big errors	0
Unknown community name	0	No such name errors	0
Illegal operation for community name supplied	0	Bad values errors	0
Encoding errors	0	General errors	0
Number of requested variables	0	Response PDUs	0
Number of altered variables	0	Trap PDUs	0
Get-request PDUs	0		
Get-next PDUs	0		
Set-request PDUs	0		

Refresh

REMOTE MONITORING

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.

The 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.

CONFIGURING RMON ALARMS

Use the Administration > RMON (Configure Global - Add - Alarm) page to define specific criteria that will generate response events. Alarms can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to rising or falling thresholds. (However, note that after an alarm is triggered it will not be triggered again until the statistical value crosses the opposite bounding threshold and then back across the trigger threshold.

CLI REFERENCES

- ◆ ["Remote Monitoring Commands" on page 807](#)

COMMAND USAGE

- ◆ If an alarm is already defined for an index, the entry must be deleted before any changes can be made.

PARAMETERS

These parameters are displayed:

- ◆ **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)
- ◆ **Sample Type** – Tests for absolute or relative changes in the specified variable.
 - **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.
- ◆ **Rising Threshold** – 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. (Range: 0-2147483647)
- ◆ **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)

- ◆ **Falling 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. (Range: 0-2147483647)
- ◆ **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)
- ◆ **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON alarm:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Alarm.
5. Enter an index number, the MIB object to be polled (etherStatsEntry.n.n), the polling interval, the sample type, the thresholds, and the event to trigger.
6. Click Apply

Figure 267: Configuring an RMON Alarm

The screenshot shows the 'Administration > RMON' configuration page. At the top, there are two dropdown menus: 'Step:' set to '1. Configure Global' and 'Action:' set to 'Add'. Below these are two radio buttons: 'Alarm' (selected) and 'Event'. The main configuration area contains several labeled input fields: 'Index (1-65535)' with value '1', 'Variable' with value '6.1', 'Interval (1-31622400)' with value '15' and a 'sec' unit, 'Sample Type' with a dropdown set to 'Delta', 'Rising Threshold (0-2147483647)' with value '100', 'Rising Event Index (0-65535)' with value '30', 'Falling Threshold (0-2147483647)' with value '1', 'Falling Event Index (0-65535)' with value '2', and 'Owner' with value 'bill'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

To show configured RMON alarms:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Alarm.

Figure 268: Showing Configured RMON Alarms

Administration > RMON

Step: 1. Configure Global Action: Show

☒ Alarm ☐ Event

RMON Alarm List Total: 28

	Index	Status	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
<input type="checkbox"/>	1	Valid	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
<input type="checkbox"/>	2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
<input type="checkbox"/>	3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
<input type="checkbox"/>	4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
<input type="checkbox"/>	5	Valid	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	

CONFIGURING RMON EVENTS

Use the Administration > RMON (Configure Global - Add - Event) page to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

CLI REFERENCES

- ◆ ["Remote Monitoring Commands" on page 807](#)

COMMAND USAGE

- ◆ If an alarm is already defined for an index, the entry must be deleted before any changes can be made.
- ◆ One default event is configured as follows:
 - event Index = 1
 - Description: RMON_TRAP_LOG
 - Event type: log & trap
 - Event community name is public
 - Owner is RMON_SNMP

PARAMETERS

These parameters are displayed:

- ◆ **Index** – Index to this entry. (Range: 1-65535)

- ◆ **Type** – Specifies the type of event to initiate:
 - **None** – No event is generated.
 - **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 ["System Log Configuration" on page 412](#)).
 - **Trap** – Sends a trap message to all configured trap managers (see ["Specifying Trap Managers" on page 462](#)).
 - **Log and Trap** – Logs the event and sends a trap message.
- ◆ **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts.

Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page (see ["Setting Community Access Strings" on page 456](#)) prior to configuring it here. (Range: 1-127 characters)
- ◆ **Description** – A comment that describes this event. (Range: 1-127 characters)
- ◆ **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON event:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Event.
5. Enter an index number, the type of event to initiate, the community string to send with trap messages, the name of the person who created this event, and a brief description of the event.
6. Click Apply

Figure 269: Configuring an RMON Event

Administration > RMON

Step: 1. Configure Global Action: Add

☐ Alarm ☒ Event

Index (1-65535) 2

Type Log and Trap

Community private

Description for software group

Owner david

Apply Revert

To show configured RMON events:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Event.

Figure 270: Showing Configured RMON Events

Administration > RMON

Step: 1. Configure Global Action: Show

☐ Alarm ☒ Event

RMON Event List Total: 4

	Index	Status	Type	Community	Description	Owner	Last Fired
<input type="checkbox"/>	1	Valid	None		None	None	00:00:00
<input type="checkbox"/>	2	Valid	Log		Log	Log	00:00:00
<input type="checkbox"/>	3	Valid	Trap	Trap	Trap	Trap	00:00:00
<input type="checkbox"/>	4	Valid	Log and Trap	Log and Trap	Log and Trap	Log and Trap	00:00:00

Delete Revert

CONFIGURING RMON
HISTORY SAMPLES

Use the Administration > RMON (Configure Interface - Add - History) page to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems. The record can be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. It can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

CLI REFERENCES

- ◆ "Remote Monitoring Commands" on page 807

COMMAND USAGE

- ◆ Each index number equates to a port on the switch.
- ◆ If history collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- ◆ 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.

For a description of the statistics displayed on the Show Details page, refer to ["Showing Port or Trunk Statistics" on page 162](#).
- ◆ The switch reserves two index entries for each port. If a default index entry is re-assigned to another port using the Add page, this index will not appear in the Show nor Show Details page for the port to which is normally assigned. For example, if control entry 15 is assigned to port 5, this index entry will be removed from the Show and Show Details page for port 8.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – The port number on the switch.
- ◆ **Index** - Index to this entry. (Range: 1-65535)
- ◆ **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800 seconds)
- ◆ **Buckets** - The number of buckets requested for this entry. (Range: 1-65536; Default: 50)

The number of buckets granted are displayed on the Show page.
- ◆ **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To periodically sample statistics on a port:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click History.
5. Select a port from the list as the data source.
6. Enter an index number, the sampling interval, the number of buckets to use, and the name of the owner for this entry.

7. Click Apply

Figure 271: Configuring an RMON History Sample

Administration > RMON

Step: 2. Configure Interface Action: Add

☒ History ☐ Statistics

Port 2

Index (1-65535) 100

Interval (1-3600) 60 sec

Buckets (1-65535) 10

Owner david

Apply Revert

To show configured RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port from the list.
5. Click History.

Figure 272: Showing Configured RMON History Samples

Administration > RMON

Step: 2. Configure Interface Action: Show

☒ History ☐ Statistics

Port 1

RMON History Port List Total: 2

	Index	Status	Interval	Requested Buckets	Granted Buckets	Owner
<input type="checkbox"/>	1	Valid	1800	8	8	
<input type="checkbox"/>	2	Valid	30	8	8	

Delete Revert

To show collected RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.

4. Select a port from the list.
5. Click History.

Figure 273: Showing Collected RMON History Samples

History Index	Sample Index	Interval Start	Octets	Packets	Broadcast Packets	Multicast Packets	Undersize Packets	Oversize Packets	Fragments	Jabbers	CRC Align Errors	Collisions	Drop Events	Network Utilization
1	1	00:00:01	756105	3218	91	894	0	0	0	0	0	0	0	0
2	71	00:35:01	21490	76	0	15	0	0	0	0	0	0	0	0
2	72	00:35:31	46521	120	0	15	0	0	0	0	0	0	0	0
2	73	00:36:01	21682	79	0	15	0	0	0	0	0	0	0	0
2	74	00:36:31	21554	77	0	15	0	0	0	0	0	0	0	0

CONFIGURING RMON STATISTICAL SAMPLES

Use the Administration > RMON (Configure Interface - Add - Statistics) page to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates.

CLI REFERENCES

- ◆ ["Remote Monitoring Commands" on page 807](#)

COMMAND USAGE

- ◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- ◆ The information collected for each entry includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – The port number on the switch.
- ◆ **Index** - Index to this entry. (Range: 1-65535)
- ◆ **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To enable regular sampling of statistics on a port:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click Statistics.
5. Select a port from the list as the data source.
6. Enter an index number, and the name of the owner for this entry
7. Click Apply

Figure 274: Configuring an RMON Statistical Sample

The screenshot shows the 'Administration > RMON' web interface. At the top, there is a breadcrumb trail 'Administration > RMON'. Below this, there are two dropdown menus: 'Step:' with '2. Configure Interface' selected, and 'Action:' with 'Add' selected. Underneath these, there are two radio buttons: 'History' (unselected) and 'Statistics' (selected). Below the radio buttons, there is a 'Port' dropdown menu with '2' selected. Further down, there are two text input fields: 'Index (1-65535)' with the value '100' entered, and 'Owner' with the value 'mary' entered. At the bottom right of the form, there are two buttons: 'Apply' and 'Revert'.

To show configured RMON statistical samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port from the list.
5. Click Statistics.

Figure 275: Showing Configured RMON Statistical Samples

The screenshot shows the 'Administration > RMON' configuration page. At the top, there is a breadcrumb trail 'Administration > RMON' and a help icon. Below this, there are two dropdown menus: 'Step: 2. Configure Interface' and 'Action: Show'. There are two radio buttons: 'History' (unselected) and 'Statistics' (selected). Below the radio buttons is a 'Port' dropdown menu set to '2'. The main content area is titled 'RMON Statistics Port List' with a 'Total: 2' indicator. It contains a table with four columns: a checkbox, 'Index', 'Status', and 'Owner'. The table has two rows of data. Below the table are 'Delete' and 'Revert' buttons.

	Index	Status	Owner
<input type="checkbox"/>	1	Valid	abc
<input type="checkbox"/>	2	Valid	test

To show collected RMON statistical samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.
4. Select a port from the list.
5. Click Statistics.

Figure 276: Showing Collected RMON Statistical Samples

The screenshot shows the 'Administration > RMON' configuration page with the 'Action' dropdown set to 'Show Details'. The 'Step' dropdown remains '2. Configure Interface'. The 'Port' dropdown is still '2'. The 'Statistics' radio button is selected. The main content area is titled 'RMON Statistics Port Details'. It displays a list of statistical metrics and their values. A 'Refresh' button is located at the bottom right.

Received Octets	9613105	Collisions	0
Received Packets	24621	Drop Events	0
Broadcast Packets	608	Frames of 64 Octets	13595
Multicast Packets	5538	Frames of 65 to 127 Octets	2606
Undersize Packets	0	Frames of 128 to 255 Octets	1222
Oversize Packets	0	Frames of 256 to 511 Octets	56
CRC Align Errors	0	Frames of 512 to 1023 Octets	2028
Jabbers	0	Frames of 1024 to 1518 Octets	5114
Fragments	0		

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.

COMMAND USAGE

- ◆ 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 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.
- ◆ There can be up to 100 candidates and 36 member switches in one cluster.
- ◆ A switch can only be a member of one cluster.
- ◆ After the Commander and Members have been configured, any switch in the cluster can be managed from the web agent by choosing the desired Member ID from the Show Member page.

CONFIGURING GENERAL SETTINGS FOR CLUSTERS

Use the Administration > Cluster (Configure Global) page to create a switch cluster.

CLI REFERENCES

- ◆ ["Switch Clustering" on page 779](#)

COMMAND USAGE

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 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.

PARAMETERS

These parameters are displayed:

- ◆ **Cluster Status** – Enables or disables clustering on the switch.
(Default: Disabled)
- ◆ **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- ◆ **IP Pool** – An “internal” IP address pool that 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. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)
- ◆ **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate. (Default: Candidate)
- ◆ **Number of Members** – The current number of Member switches in the cluster.
- ◆ **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

WEB INTERFACE

To configure a switch cluster:

1. Click Administration, Cluster.
2. Select Configure Global from the Step list.
3. Set the required attributes for a Commander or a managed candidate.
4. Click Apply

Figure 277: Configuring a Switch Cluster

The screenshot shows a web interface for configuring a switch cluster. At the top, it says "Administration > Cluster". Below that is a "Step:" dropdown menu with "1. Configure Global" selected. The main configuration area contains several settings:

Cluster Status	<input checked="" type="checkbox"/> Enabled
Commander Status	<input checked="" type="checkbox"/> Enabled
IP Pool	<input type="text" value="10.254.254.1"/>
Role	Commander
Number of Members	2
Number of Candidates	3

At the bottom right, there are two buttons: "Apply" and "Revert".

CLUSTER MEMBER CONFIGURATION Use the Administration > Cluster (Configure Member - Add) page to add Candidate switches to the cluster as Members.

CLI REFERENCES

- ◆ "Switch Clustering" on page 779

PARAMETERS

These parameters are displayed:

- ◆ **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- ◆ **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

WEB INTERFACE

To configure cluster members:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Add from the Action list.
4. Select one of the cluster candidates discovered by this switch, or enter the MAC address of a candidate.
5. Click Apply.

Figure 278: Configuring a Cluster Members

The screenshot shows the 'Administration > Cluster' web interface. At the top, there's a breadcrumb 'Administration > Cluster'. Below it, a 'Step:' dropdown is set to '2. Configure Member' and an 'Action:' dropdown is set to 'Add'. The main form area has two sections: 'Member ID (1-36)' with an empty text input field, and 'MAC Address' with two radio buttons. The first radio button, labeled 'Candidate', is selected and has a dropdown menu showing '11-22-33-44-55-11'. The second radio button is unselected and has an empty text input field. At the bottom right of the form are two buttons: 'Apply' and 'Revert'.

To show the cluster members:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Show from the Action list.

Figure 279: Showing Cluster Members

Administration > Cluster

Step: 2. Configure Member Action: Show

Cluster Member List Total: 2

<input type="checkbox"/>	Member ID	Role	IP Address	MAC Address	Description
<input type="checkbox"/>	1	Active Member	10.254.254.2	70-72-CF-6D-F8-E0	ECS4510-28P
<input type="checkbox"/>	2	Member To Be	10.254.254.3	70-20-CF-6D-FB-A0	ECS4510-28F

Delete Revert

To show cluster candidates:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Show Candidate from the Action list.

Figure 280: Showing Cluster Candidates

Administration > Cluster

Step: 2. Configure Member Action: Show Candidate

Cluster Candidate List Total: 4

Role	MAC Address	Description
Candidate	11-22-33-44-55-11	ECS4510-28T
Active Member	11-22-33-44-55-22	ECS4510-28T
Candidate	11-22-33-44-55-33	ECS4510-28T
Candidate	11-22-33-44-55-44	ECS4510-28T

Clear

MANAGING CLUSTER MEMBERS

Use the Administration > Cluster (Show Member) page to manage another switch in the cluster.

CLI REFERENCES

- ◆ ["Switch Clustering" on page 779](#)

PARAMETERS

These parameters are displayed:

- ◆ **Member ID** – The ID number of the Member switch. (Range: 1-36)
- ◆ **Role** – Indicates the current status of the switch in the cluster.
- ◆ **IP Address** – The internal cluster IP address assigned to the Member switch.
- ◆ **MAC Address** – The MAC address of the Member switch.
- ◆ **Description** – The system description string of the Member switch.

- ◆ **Operate** – Remotely manage a cluster member.

WEB INTERFACE

To manage a cluster member:

1. Click Administration, Cluster.
2. Select Show Member from the Step list.
3. Select an entry from the Cluster Member List.
4. Click Operate.

Figure 281: Managing a Cluster Member

Administration > Cluster					
Step: 3. Show Member					
Cluster Member List Total: 2					
	Member ID	Role	IP Address	MAC Address	Description
<input checked="" type="radio"/>	1	Active Member	10.254.254.2	11-22-33-44-55-33	ECS4510-28T
<input type="radio"/>	2	Candidate	10.254.254.3	11-22-33-44-55-77	ECS4510-28T

Operate

ETHERNET RING PROTECTION SWITCHING



NOTE: Information in this section is based on ITU-T G.8032/Y.1344.

The ITU G.8032 recommendation specifies a protection switching mechanism and protocol for Ethernet layer network rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in G.8032 achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

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. An Ethernet ring built using ERPS can provide resilience at a lower cost and than that provided by SONET or EAPS rings.

ERPS is more economical than EAPS in that only one physical link is required between each node in the ring. However, since it can tolerate only one break in the ring, it is not as robust as EAPS. ERPS supports up to 255 nodes in the ring structure. ERPS requires a higher convergence time when more than 16 nodes are used, but should always run under than 500 ms.

Operational Concept

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked to traffic. One designated node, the RPL owner, is responsible for blocking traffic over the RPL. When a ring failure occurs, the RPL owner is responsible for unblocking the RPL, allowing this link to be used for traffic.

Ring nodes may be in one of two states:

Idle – normal operation, no link/node faults detected in ring

Protection – Protection switching in effect after identifying a signal fault

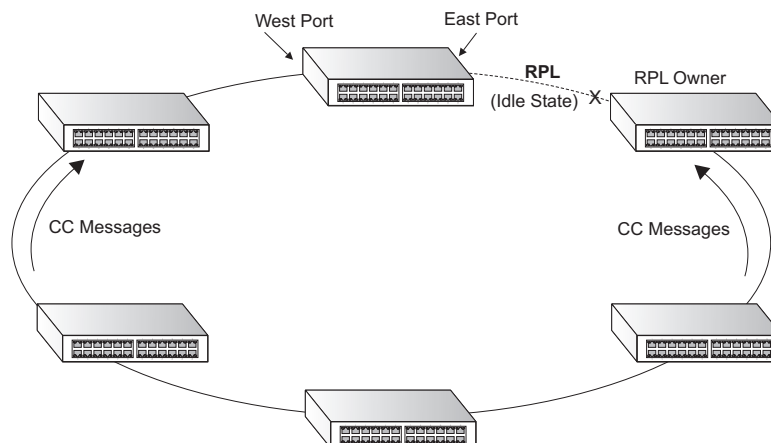
In Idle state, the physical topology has all nodes connected in a ring. The logical topology guarantees that all nodes are connected without a loop by blocking the RPL. Each link is monitored by its two adjacent nodes using Connectivity Fault Management (CFM) protocol messages.

Protection switching (opening the RPL to traffic) occurs when a signal failure message generated by the Connectivity Fault Management (CFM) protocol is declared on one of the ring links, and the detected failure has a higher priority than any other request; or a Ring – Automatic Protection Switching protocol request (R-APS, as defined in Y.1731) is received which has a higher priority than any other local request.

A link/node failure is detected by the nodes adjacent to the failure. These nodes block the failed link and report the failure to the ring using R-APS (SF) messages. This message triggers the RPL owner to unblock the RPL, and all nodes to flush their forwarding database. The ring is now in protection state, but it remains connected in a logical topology.

When the failed link recovers, the traffic is kept blocked on the nodes adjacent to the recovered link. The nodes adjacent to the recovered link transmit R-APS (NR - no request) message indicating they have no local request. When the RPL owner receives an R-APS (NR) message it starts the Wait-To-Recover (WTR) timer. Once WTR timer expires, the RPL owner blocks the RPL and transmits an R-APS (NR, RB - ring blocked) message. Nodes receiving this message flush the forwarding database and unblock their previously blocked ports. The ring is now returned to Idle state.

Figure 282: ERPS Ring Components



Multi-ring/Ladder Network – ERPSv2 also supports multipoint-to-multipoint connectivity within interconnected rings, called a “multi-ring/ladder network” topology. This arrangement consists of conjoined rings connected by one or more interconnection points, and is based on the following criteria:

- ◆ The R-APS channels are not shared across Ethernet Ring interconnections.
- ◆ On each ring port, each traffic channel and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet Ring Protection Control Process (ERP Control Process) of only one ring.
- ◆ Each Major Ring or Sub-Ring must have its own RPL.

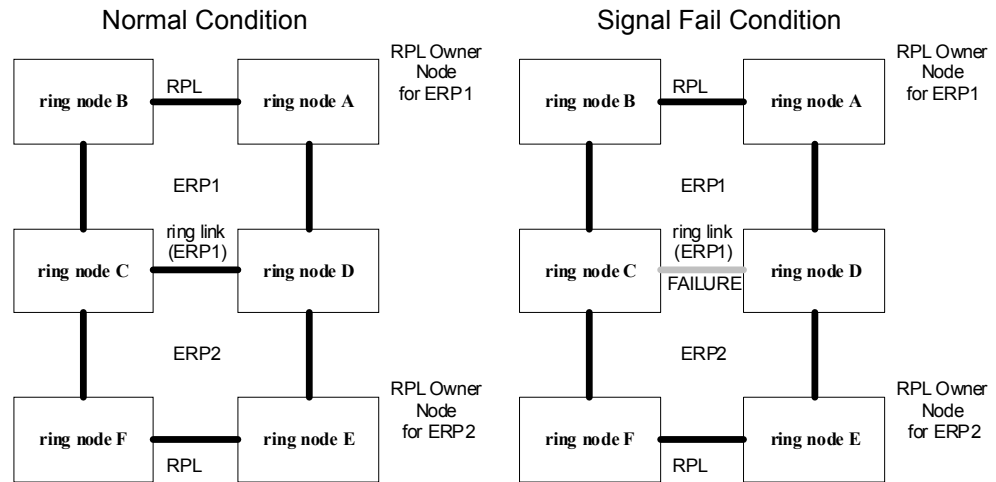
[Figure 283 on page 488](#) (Normal Condition) depicts an example of a multi-ring/ladder network. If the network is in normal operating condition, the RPL owner node of each ring blocks the transmission and reception of traffic over the RPL for that ring. This figure presents the configuration when no failure exists on any ring link.

In the figure for the Normal Condition there are two interconnected rings. Ring ERP1 is composed of ring nodes A, B, C and D and the ring links between these nodes. Ring ERP2 is composed of ring nodes C, D, E and F and the ring links C-to-F, F-to-E, E-to-D. The ring link between D and C is used for traffic on rings ERP1 and ERP2. On their own ERP2 ring links do not form a closed loop. A closed loop may be formed by the ring links of ERP2 and the ring link between the interconnection nodes that is controlled by ERP1. ERP2 is a sub-ring. Ring node A is the RPL owner node for ERP1, and ring node E is the RPL owner node for ERP2. These ring nodes (A and E) are responsible for blocking the traffic channel on the RPL for ERP1 and ERP2 respectively. There is no restriction on which ring link on an ring may be set as the RPL. For example the RPL of ERP1 could be set as the link between ring node C and D.

Ring nodes C and D, that are common to both ERP1 and ERP2, are called interconnection nodes. The ring link between the interconnection nodes are controlled and protected by the ring it belongs to. In the example for the Normal Condition, the ring link between ring nodes C and D is part of ERP1, and, as such, are controlled and protected by ERP1. Ethernet characteristic information traffic corresponding to the traffic channel may be transferred over a common Ethernet connection for ERP1 and ERP2 through the interconnection nodes C and D. Interconnection nodes C and D have separate ERP Control Processes for each Ethernet Ring.

[Figure 283 on page 488](#) (Signal Fail Condition) illustrates a situation where protection switching has occurred due to an SF condition on the ring link between interconnection nodes C and D. The failure of this ring link triggers protection only on the ring to which it belongs, in this case ERP1. The traffic and R-APS channels are blocked bi-directionally on the ports where the failure is detected and bi-directionally unblocked at the RPL connection point on ERP1. The traffic channels remain bi-directionally blocked at the RPL connection point on ERP2. This prevents the formation of a loop.

Figure 283: Ring Interconnection Architecture (Multi-ring/Ladder Network)



Configuration Guidelines for ERPS

1. Create an ERPS ring ([Configure Domain – Add](#)): The ring name is used as an index in the G.8032 database.
2. Configure the east and west interfaces ([Configure Domain – Configure Details](#)): Each node on the ring connects to it through two ring ports. Configure one port connected to the next node in the ring to the east (or clockwise direction) and another port facing west in the ring.
3. Configure the RPL owner ([Configure Domain – Configure Details](#)): Configure one node in the ring as the Ring Protection Link (RPL) owner. 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 ([Configure Domain – Configure Details](#)): Set the Guard timer to prevent ring nodes from receiving outdated R-APS messages, the Hold-off timer to filter out intermittent link faults, and the WTR timer to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.
5. Configure the ERPS Control VLAN ([Configure Domain – Configure Details](#)): Specify the control VLAN (CVLAN) 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 ([Configure Global](#)): Before enabling a ring as described in the next step, first globally enable ERPS on the switch. If ERPS has not yet been enabled or has been disabled, no ERPS rings will work.
7. Enable an ERPS ring ([Configure Domain – Configure Details](#)): Before an ERPS ring can work, it must be enabled. 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. A ring can be stopped by disabling the Admin Status on any node.
8. Display ERPS status information ([Configure Domain – Show](#)): Display ERPS status information for all configured rings.

Configuration Limitations for ERPS

The following configuration limitations apply to ERPS:

- ◆ The switch supports up to six ERPS rings – each ring must have one Control VLAN, and at most 255 Data VLANs.
- ◆ Ring ports can not be a member of a trunk, nor an LACP-enabled port.
- ◆ Dynamic VLANs are not supported as protected data ports.
- ◆ Exclusive use of STP or ERPS on any port.
- ◆ The switch takes about 350 ms to detect link-up on 1000Base-T copper ports, so the convergence time on this port type is more than 50 ms.
- ◆ One VLAN must be added to an ERPS domain as the CVLAN. This can be designated as any VLAN, other than the management VLAN. The CVLAN should only contain ring ports, and must not be configured with an IP address.

ERPS GLOBAL CONFIGURATION

Use the Administration > ERPS (Configure Global) page to globally enable or disable ERPS on the switch.

CLI REFERENCES

- ◆ ["erps" on page 1089](#)

PARAMETERS

These parameters are displayed:

- ◆ **ERPS Status** – Enables ERPS on the switch. (Default: Disabled)
ERPS must be enabled globally on the switch before it can be enabled on an ERPS ring (by setting the Admin Status on the [Configure Domain – Configure Details](#) page).

WEB INTERFACE

To globally enable ERPS on the switch:

1. Click Administration, ERPS.
2. Select Configure Global from the Step list.
3. Mark the ERPS Status check box.
4. Click Apply.

Figure 284: Setting ERPS Global Status



The screenshot shows a web interface for configuring ERPS. At the top, it says 'Administration > ERPS'. Below that, there's a 'Step:' dropdown menu set to '1. Configure Global'. Underneath, the 'ERPS Status' is shown with a checked checkbox and the text 'Enabled'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

ERPS RING CONFIGURATION

Use the Administration > ERPS (Configure Domain) pages to configure ERPS rings.

CLI REFERENCES

- ◆ ["ERPS Commands" on page 1087](#)

COMMAND USAGE

Ring Initialization

An ERPS ring containing one Control VLAN and one or more protected Data VLANs must be configured, and the global ERPS function enabled on the switch (see ["ERPS Global Configuration" on page 489](#)) before a ring can start running. Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter the active state.

Limitations

When configuring a ring port, note that these ports cannot be part of a spanning tree, nor can they be members of a static or dynamic trunk.

PARAMETERS

These parameters are displayed:

Add

- ◆ **Domain Name** – Name of an ERPS ring. (Range: 1-12 characters)
- ◆ **Domain ID** – ERPS ring identifier used in R-APS messages. (Range: 1-255)

Show

- ◆ **Domain Name** – Name of a configured ERPS ring.
- ◆ **ID** – ERPS ring identifier used in R-APS messages.
- ◆ **Admin Status** – Shows whether ERPS is enabled on the switch.
- ◆ **Ver** – Shows the ERPS version.
- ◆ **MEG Level** – The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
- ◆ **Control VLAN** – Shows the Control VLAN ID.
- ◆ **Node 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 node type as None, RPL Owner or RPL Neighbor.
- ◆ **Revertive** – Shows if revertive or non-revertive recovery is selected.
- ◆ **W/E** – Shows information on the west and east ring port for this node.
- ◆ **West Port** – Shows the west ring port for this node.
- ◆ **East Port** – Shows the east ring port for this node.
- ◆ **Interface** – The port or trunk which is configured as a ring port.
- ◆ **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.

Configure Details

- ◆ **Domain Name** – Name of a configured ERPS ring. (Range: 1-12 characters)

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.
- ◆ **Domain ID** – ERPS ring identifier used in R-APS messages. (Range: 1-255; Default: None)

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 for the R-APS Def MAC parameter, then the Domain ID will be used in R-APS PDUs.
- ◆ **Admin Status** – Activates the current ERPS ring. (Default: Disabled)

Before enabling a ring, the global ERPS function should be enabled see ("[ERPS Global Configuration](#)" on page 489), the east and west ring ports configured on each node, the RPL owner specified, and the control VLAN configured.

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.
- ◆ **Version** – Specifies compatibility with the following ERPS versions:
 - 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. (This is the default setting.)

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 R-APS Def MAC parameter has no effect.

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

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.

- ◆ **Control VLAN** – A dedicated VLAN used for sending and receiving E-APS protocol messages. (Range: 1-4093)

Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN (see ["Configuring VLAN Groups" on page 196](#)), add the ring ports for the east and west interface as tagged members to this VLAN (see ["Adding Static Members to VLANs" on page 199](#)), and then use this parameter 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, the configuration of the control VLAN cannot be modified. Use the Admin Status parameter to stop the ERPS ring before making any configuration changes to the control VLAN.

- ◆ **Node State** – Refer to the parameters for the Show page.
- ◆ **Node Type** – Shows ERPS node type as one of the following:
 - **None** – Node is neither Ring Protection Link (RPL) owner nor neighbor. (This is the default setting.)
 - **RPL Owner** – Specifies a ring node to be the RPL owner.

- 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 Forced Switch or Manual Switch commands on the Configure Operation page).
- The east and west connections to the ring must be specified for all ring nodes. When this switch is configured as the RPL owner, the west ring port is automatically set as being connected to the RPL.
- **RPL Neighbor** – Specifies a ring node to be the RPL neighbor.
 - 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. 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.
- ◆ **Revertive** – Sets the method of recovery to Idle State through revertive or non-revertive mode. (Default: Enabled)
 - 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 (FS), and Manual Switch (MS) states are basically the same. Non-revertive behavior requires the RPL to be restored from Protection state to Idle state using the Clear command (Configure Operation page).
 - 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 Clear command (Configure Operation page) 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 – A Forced Switch command is removed by issuing the Clear command (Configure Operation page) 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 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 as follows:
 - 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.
- Recovery with non-revertive mode is handled as follows:
 - 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 Clear command (Configure Operation page) 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 – A Manual Switch command is removed by issuing the Clear command (Configure Operation page) 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 as follows:
 - 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 as follows:
 - 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 Clear command (Configure Operation page) 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.

◆ **Major Domain** – The ERPS ring used for sending control packets.

This switch can support up to six rings. However, ERPS control packets can only be sent on one ring. This parameter 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 always the west port. 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. The major domain therefore cannot be set if the east port is already configured.

◆ **Node ID** – 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: CPU MAC address)

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.

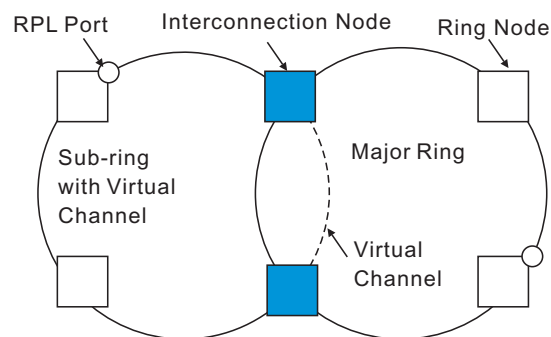
The node identifier may also be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

◆ **R-APS with VC** – Configures an R-APS virtual channel to connect two interconnection points on a sub-ring, allowing ERPS protocol traffic to be tunneled across an arbitrary Ethernet network. (Default: Enabled)

- 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.

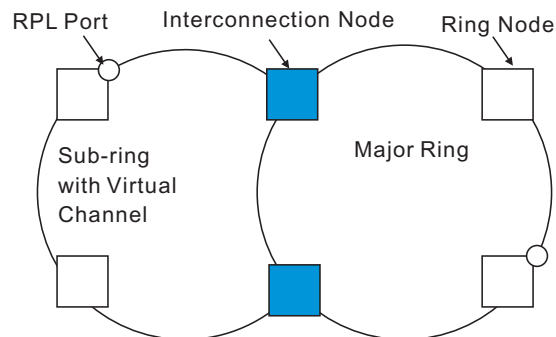
Figure 285: Sub-ring with Virtual Channel



- 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 286: Sub-ring without Virtual Channel



- ◆ **R-APS Def MAC** – Sets the switch’s MAC address to be used as the node identifier in R-APS messages. (Default: Enabled)

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]

- ◆ **Propagate TC** – Enables propagation of topology change messages from a secondary ring to the primary ring. (Default: Disabled)

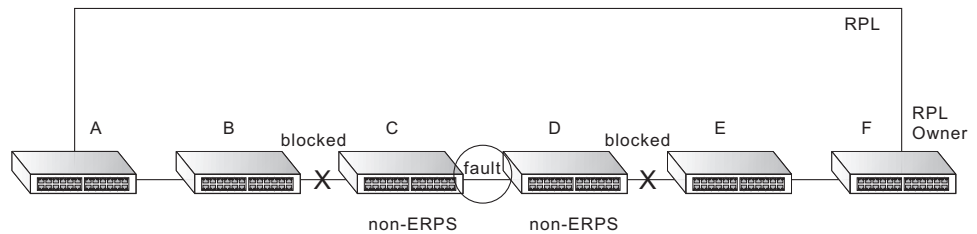
When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through 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.

- ◆ **Non-ERPS Device Protection** – Sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through Signal Fault messages. (Default: Disabled)

- 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 ["Connectivity Fault Management" on page 510](#). 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.



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.

- ◆ **Holdoff Timer** – 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)

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.

- ◆ **Guard Timer** – 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)

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.

- ◆ **WTB Timer** – The Wait to Block (WTB) timer is used when clearing Forced Switch (FS) and Manual Switch (MS) commands. As multiple FS commands are allowed to co-exist in a ring, the WTB timer ensures that clearing of a single FS command does not trigger re-blocking of the RPL. When clearing an MS command, the WTB timer prevents the formation of a closed loop due to possible a timing anomaly where the RPL owner node receives an outdated remote MS request during the recovery process.

When recovering from an FS or MS command, the delay timer must be long enough to receive any latent remote FS or MS commands. This delay timer called the WTB timer is defined to be 5 seconds longer than the guard timer. This is enough time to allow a reporting ring node to transmit two R-APS messages and allow the ring to identify the latent condition.

This delay timer is activated on the RPL owner node. When the relevant delay timer expires, the RPL owner node initiates the reversion process by transmitting an R-APS (NR, RB) message. The delay timer, (i.e., WTR or WTB) is deactivated when any higher priority request pre-empts this delay timer.

The delay timers (i.e. WTR and WTB) may be started and stopped by the system. A request to start running the delay timer does not restart the delay timer. A request to stop the delay timer stops the delay timer and resets its value. The Clear command (Configure Operation page) can be used to stop the delay timer.

- ◆ **WTR Timer** – 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)

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.

- ◆ **WTB Expire** – The time before the wait-to-block timer expires.
- ◆ **WTR Expire** – The time before the wait-to-restore timer expires.

- ◆ **West/East** – Connects to next ring node to the west/east.
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.
- ◆ **Interface** – The port or trunk attached to the west or east ring port.
Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk.
- ◆ **Port State** – Once configured, this field shows the operational state of the ring ports for this node:
 - 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.
- ◆ **Local SF** – Shows if a signal fault exists 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** – Specifies the CCM MEPs used to monitor the link on a ring node.

If a MEP is used to monitor the link status of an ERPS node with CFM continuity check messages, then the MEG Level parameter on this configuration page must match the authorized maintenance level of the CFM domain to which the specified MEP belongs. (See "[Configuring CFM Maintenance Domains](#)" on page 517.)

To ensure complete monitoring of a ring node, specify the CFM MEPs used to monitor both the east and west ports of the ring node.

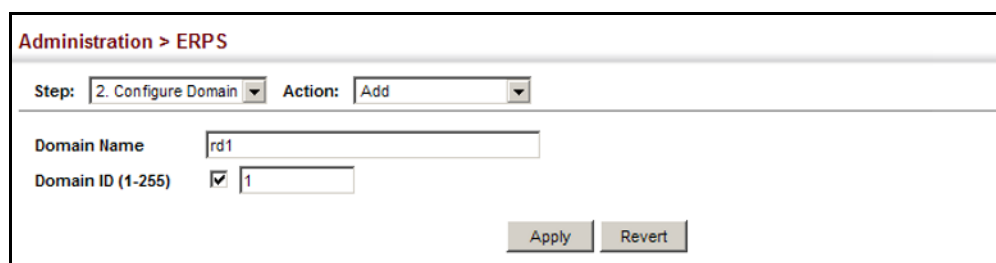
If CFM determines that a MEP node which has been configured to monitor a ring port with this command has gone down, this information is passed to ERPS, which in turn processes it as a ring node failure. For more information on how ERPS recovers from a node failure, refer to the description of the Revertive parameter on this configuration page.
- ◆ **RPL** – If node is connected to the RPL, this shows by which interface.

WEB INTERFACE

To create an ERPS ring:

1. Click Administration, ERPS.
2. Select Configure Domain from the Step list.
3. Select Add from the Action list.
4. Enter a name and optional identifier for the ring.
5. Click Apply.

Figure 287: Creating an ERPS Ring



The screenshot shows a web interface for configuring ERPS. The breadcrumb navigation at the top reads "Administration > ERPS". Below this, there are two dropdown menus: "Step:" set to "2. Configure Domain" and "Action:" set to "Add". The main configuration area contains two fields: "Domain Name" with the text "rd1" and "Domain ID (1-255)" with a checked checkbox and the value "1". At the bottom right of the form are two buttons: "Apply" and "Revert".

To configure the ERPS parameters for a ring:

1. Click Administration, ERPS.
2. Select Configure Domain from the Step list.
3. Select Configure Details from the Action list.
4. Configure the ERPS parameters for this node. Note that spanning tree protocol cannot be configured on the ring ports, nor can these ports be members of a static or dynamic trunk. And the control VLAN must be unique for each ring. Adjust the protocol timers as required. The RPL owner must be set on one of the rings. And the administrative status enabled once all of the other settings have been entered.
5. Click Apply.

Figure 288: Creating an ERPS Ring

Administration > ERPS

Step: 2. Configure Domain Action: Configure Details

Domain Name: rd1

Domain ID: 1

Admin Status: ☒ Enabled

Version: 2

MEG Level (0-7): 1

Control VLAN: ☒ 2

Node State: Idle

Node Type: RPL Owner

Revertive: ☒ Enabled

Major Domain: ☐ ☐

Node ID: 00-E0-0C-00-00-FD

R-APS with VC: ☒ Enabled

R-APS Def MAC: ☒ Enabled

Propagate TC: ☐ Enabled

Non-ERPS Dev Protect: ☐ Enabled

Holdoff Timer (0-10000): 0 ms

Guard Timer (10-2000): 500 ms

WTB Timer: 5500 ms

WTR Timer (5-12): 5 min

WTB Expire

WTR Expire

West: ☒ Enabled

Interface: Eth 1/10

Port State: Blocking

Local SF: No

Local FS: No

Local MS: No

MEP (1-8191): ☐

RPL: Yes

East: ☒ Enabled

Interface: Eth 1/12

Port State: Forwarding

Local SF: No

Local FS: No

Local MS: No

MEP (1-8191): ☐

RPL: No

Apply Revert

To show the configure ERPS rings:

1. Click Administration, ERPS.
2. Select Configure Domain from the Step list.
3. Select Show from the Action list.

Figure 289: Showing Configured ERPS Rings

Administration > ERPS

Step: 2. Configure Domain Action: Show

Domain List Total: 1

	Domain Name	ID	Admin Status	Ver	MEG Level	Control VLAN	Node State	Type	Revertive	W/E	Interface	Port State	Local SF	Local FS	Local MS	MEP	RPL
<input type="checkbox"/>	rd1	1	Enabled	2	1	2	Idle	RPL Owner	Yes	West	Eth 1/10	Blocking	No	No	No		Yes
										East	Eth 1/12	Forwarding	No	No	No		No

Delete Revert

ERPS FORCED AND MANUAL MODE OPERATIONS

Use the Administration > ERPS (Configure Operation) page to block a ring port using Forced Switch or Manual Switch commands.

CLI REFERENCES

- ◆ "erps forced-switch" on page 1109
- ◆ "erps manual-switch" on page 1111
- ◆ "erps clear" on page 1109

PARAMETERS

These parameters are displayed:

- ◆ **Domain Name** – Name of a configured ERPS ring.
- ◆ **Operation** – Specifies a Forced Switch (FS) or Manual Switch (MS) operation on the east or west ring port.
 - **Forced Switch** – Blocks specified ring port. (Options: West or East)
 - 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 FS command triggers protection switching as follows:
 - a. The ring node where an FS 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 FS 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 32 on page 507](#)). 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 a 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 32: 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 Revertive parameter.
- 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.

- **Manual Switch** – Blocks specified ring port, in the absence of a failure or an FS command. (Options: West or East)
 - 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 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 32 on page 507](#)). 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.

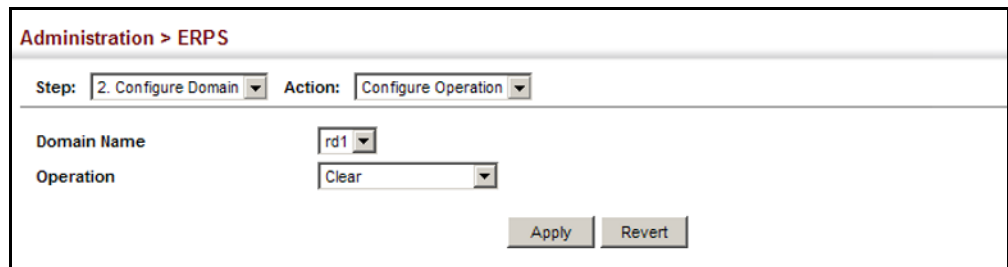
- c. An ring node with a local manual switch command that receives an R-APS message or a local request of higher priority than R-APS (MS) clear its manual switch request. The ring node then processes the new higher priority request.
- Recovery for manual switching under revertive and non-revertive mode is described under the Revertive parameter.
- **Clear** – 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.
- 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 a Clear command to remove the forced switch command on the node where a local forced switch command is active.
 2. Issue a Clear command on the RPL owner node to trigger the reversion.
- The 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 Revertive parameter. (See the Command Usage section under ["ERPS Ring Configuration" on page 490.](#))

WEB INTERFACE

To block a ring port:

1. Click Administration, ERPS.
2. Select Configure Domain from the Step list.
3. Select Configure Operation from the Action list.
4. Select the domain name from the drop-down list.
5. Specify a Forced Switch, Manual Switch, or Clear operation.
6. Click Apply.

Figure 290: Blocking an ERPS Ring Port



Administration > ERPS

Step: 2. Configure Domain Action: Configure Operation

Domain Name rd1

Operation Clear

Apply Revert

CONNECTIVITY FAULT MANAGEMENT

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).

This switch supports functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also supports fault detection through continuity check messages for all known maintenance points, and cross-check messages which are used to verify a static list of remote maintenance points located on other devices (in the same maintenance association) against those found through continuity check messages. Fault verification is supported using loop back messages, and fault isolation with 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.

Key Components of CFM

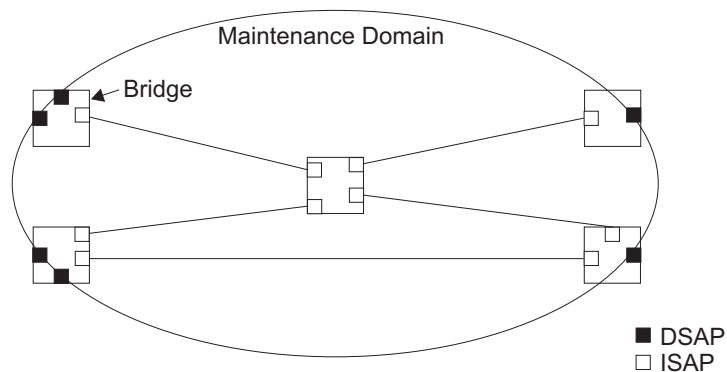
CFM provides restricted management access to each Service Instance using a structured conceptual network based on these components:

- ◆ A Maintenance Domain defines a part of the network controlled by a single operator, and supports management access to the domain through Domain Service Access Points (DSAPs) configured on the domain boundary, as well as connectivity testing between these DSAPs.
- ◆ A Maintenance Association (MA) contains the DSAPs for an individual Service Instance. DSAPs are the primary maintenance points used to monitor connectivity across a maintenance domain, and are the entry points to the paths which interconnect the access points allocated to a service instance.

- ◆ A Maintenance Level allows maintenance domains to be nested in a hierarchical fashion, providing access to the specific network portions required by each operator. Domains at lower levels may be either hidden or exposed to operators managing domains at a higher level, allowing either coarse or fine fault resolution.
- ◆ Maintenance End Points (MEPs) which provide full CFM access to a Service Instance (i.e., a specific MA), and Maintenance Intermediate Points (MIPs) which are passive entities that merely validate received CFM messages, or respond to link trace and loop back requests. MIPs are the interconnection points that make up all possible paths between the DSAPs within an MA, and may also include interconnection points in lower-level domains if exposed by CFM settings.

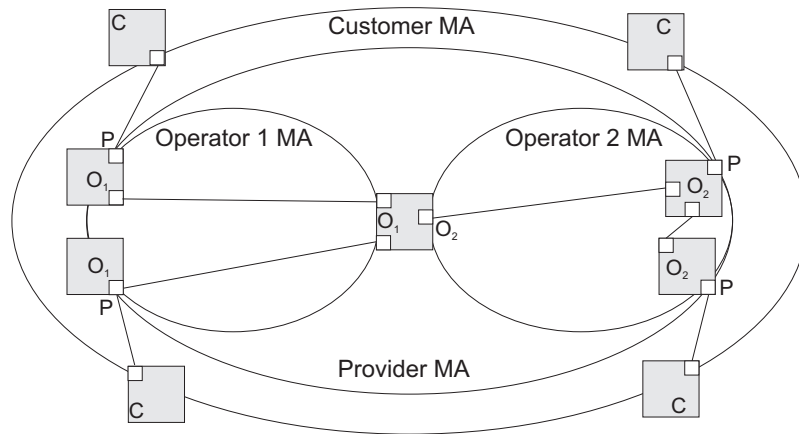
The following figure shows a single Maintenance Domain, with DSAPs located on the domain boundary, and Internal Service Access Points (ISAPs) inside the domain through which frames may pass between the DSAPs.

Figure 291: Single CFM Maintenance Domain



The figure below shows four maintenance associations contained within a hierarchical structure of maintenance domains. At the innermost level, there are two operator domains which include access points marked "O₁" and "O₂" respectively. The users of these domains can see their respective MEPs as well as all the MIPs within their domains. There is a service provider domain at the second level in the hierarchy. From the service provider's view, the access points marked "P" are visible, and all access points within the operator domains have also been made visible as MIPs according to common practice. And finally, there is a customer domain at the top of the hierarchy. Users at this level can only see the access points marked "C" on the outer domain boundary. Again, normal practice is to hide the internal structure of the network from outsiders to reduce security risks.

Figure 292: Multiple CFM Maintenance Domains



Note that the Service Instances within each domain shown above are based on a unique maintenance association for the specific users, distinguished by the domain name, maintenance level, maintenance association's name, and assigned VLAN.

Basic CFM Operations

CFM uses standard Ethernet frames for sending protocol messages. Both the source and destination address for these messages are based on unicast or multicast MAC addresses, and therefore confined to a single Layer 2 CFM service VLAN. For this reason, the transmission, forwarding, and processing of CFM frames is performed by bridges, not routers. Bridges that do not recognize CFM messages forward them as normal data. There are three basic types of CFM messages, including continuity check, link trace, and loop back.

Continuity check messages (CCMs) are multicast within a single Service Instance (i.e., a specific MA), allowing MEPs to discover other MEPs within the same MA, and MIPs to discover MEPs. Connectivity faults are indicated when a known MEP stops sending CCMs, or a remote MEP configured in a static list does not come up. Configuration errors, such as a cross-connect between different MAs, are indicated when a CCM is received with an incorrect MA identifier or maintenance level.

Loop back messages are used for fault verification. These messages can be sent using the MAC address of any destination MEP within the same MA. If the target MEP's identifier has been discovered through CCM messages, then a loop back message can also be sent using the MEPs identifier. A reply indicates that the destination is reachable.

Link trace messages are used for fault verification. These messages are multicast frames sent out to track the hop-by-hop path to a target MEP within the same MA. Responses provide information on the ingress, egress, and relay action taken at each hop along the path, providing vital information about connectivity problems. Responses allow the sender to discover all of the maintenance points that would be traversed by a data frame sent to the target MAC address.

SNMP traps can also be configured to provide an automated method of fault notification. If the fault notification generator detects one or more defects within the configured time period, and fault alarms are enabled, a corresponding trap will be sent. No further fault alarms are sent until the fault notification generator has been reset by the passage of a configured time period without detecting any further faults. Upon receiving a fault alarm, you should inspect the related SNMP objects for the reporting MEP, diagnose the fault, correct it, and re-examine the MEP's SNMP objects to see whether the fault notification generator has been reset.

Configuration Guidelines

1. Configure the maintenance domains with the MD List (see ["Configuring CFM Maintenance Domains"](#)).
2. Configure the maintenance associations with MA List (see ["Configuring CFM Maintenance Associations"](#)).
3. Configure the local maintenance end points (MEPs) which will serve as the domain service access points for the specified maintenance association using the MEP List (see ["Configuring CFM Maintenance Associations"](#)).
4. Enter a static list of MEPs assigned to other devices within the same maintenance association using the Remote MEP List (see ["Configuring Remote Maintenance End Points"](#)). 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 using the Configure Global screen (see ["Configuring Global Settings for CFM"](#)).
6. Enable CFM on the local MEPs using the Configure Interface screen (see ["Configuring Interfaces for CFM"](#)).
7. Enable continuity check and cross-check operations, and configure AIS parameters using the Configure MA – Configure Details screen (see ["Configuring CFM Maintenance Associations"](#)).

Other configuration changes may be required for your particular environment, such as adjusting the interval at which continuity check messages are sent (see ["Configuring CFM Maintenance Associations"](#)), or setting the start-up delay for the cross-check operation (see ["Configuring Global Settings for CFM"](#)). You can also enable SNMP traps for events discovered by continuity check messages or cross-check messages (see ["Configuring Global Settings for CFM"](#)).

CONFIGURING GLOBAL SETTINGS FOR CFM

Use the Administration > CFM (Configure Global) page to configure global settings for CFM, such as enabling the CFM process on the switch, setting the start-up delay for cross-check operations, configuring parameters for the link trace cache, and enabling traps for events discovered by continuity check messages or cross-check messages.

CLI REFERENCES

- ◆ ["CFM Commands" on page 1295](#)

PARAMETERS

These parameters are displayed:

Global Configuration

- ◆ **CFM Status** – Enables CFM processing globally on the switch. (Default: Enabled)

To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to enabling CFM processing globally on the switch. Specifically, the maintenance domains, maintenance associations, and maintenance end-points (MEPs) should be configured on each participating bridge using the Configure MD page (see ["Configuring CFM Maintenance Domains"](#)), Configure MA page (see ["Configuring CFM Maintenance Associations"](#)), and the Configure MEP page (see ["Configuring Maintenance End Points"](#)).

When CFM is enabled, hardware resources are allocated for CFM processing.

- ◆ **MEP Cross Check Start Delay** – Sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation. (Range: 1-65535 seconds; Default: 10 seconds)

This parameter sets the time to wait for a remote MEP to come up, and the switch starts cross-checking the list of statically configured remote MEPs in the local maintenance domain (Configure Remote MEP page, see ["Configuring Remote Maintenance End Points"](#)) against the MEPs learned through continuity check messages (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 (see ["Configuring CFM Maintenance Associations"](#)).

Link Trace Cache Settings

- ◆ **Link Trace Cache** – Enables caching of CFM data learned through link trace messages. (Default: Enabled)

A linktrace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a linktrace reply, up to the point at which the linktrace message reaches its destination or can no longer be forwarded.

Use this command attribute to enable the link trace cache to store the results of link trace operations initiated on this device. Use the CFM Transmit Link Trace page (see ["Transmitting Link Trace Messages"](#)) to transmit a linktrace message.

Linktrace 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 (see ["Displaying Fault Notification Settings"](#)).

- ◆ **Link Trace Cache Hold Time** – The hold time for CFM link trace cache entries. (Range: 1-65535 minutes; Default: 100 minutes)

Before setting the aging time for cache entries, the cache must first be enabled in the Linktrace Cache attribute field.

- ◆ **Link Trace Cache Size** – The maximum size for the link trace cache. (Range: 1-4095 entries; Default: 100 entries)

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, or purged (see ["Displaying Fault Notification Settings"](#)).

Continuity Check Errors

- ◆ **Connectivity Check Config** – Sends a trap if this device receives a continuity check message (CCM) with the same maintenance end point identifier (MPID) as its own but with a different source MAC address, indicating that a CFM configuration error exists.
- ◆ **Connectivity Check 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.
- ◆ **Connectivity Check MEP Down** – Sends a trap if this device loses connectivity with a remote maintenance end point (MEP), or connectivity has been restored to a remote MEP which has recovered from an error condition.
- ◆ **Connectivity Check 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.

MEP Up traps are suppressed when cross-checking of MEPs is enabled²⁰ because cross-check traps include more detailed status information.

Cross-check Errors

- ◆ **Cross Check MA Up** – Sends a trap when all remote MEPs in an MA come up.
An MA Up trap is sent if cross-checking is enabled²⁰, and a CCM is received from all remote MEPs configured in the static list for this maintenance association²¹.
- ◆ **Cross Check 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.
A MEP Missing trap is sent if cross-checking is enabled²⁰, and no CCM is received for a remote MEP configured in the static list²¹.

20. Cross-checking must be enabled for this type of trap to be reported (see ["Configuring CFM Maintenance Associations"](#)).

21. See ["Configuring Maintenance End Points"](#).

- ◆ **Cross Check MEP Unknown** – Sends a trap if an unconfigured MEP comes up.

A MEP Unknown trap is sent if cross-checking is enabled²⁰, and a CCM is received from a remote MEP that is not configured in the static list²¹.

WEB INTERFACE

To configure global settings for CFM:

1. Click Administration, CFM.
2. Select Configure Global from the Step list.
3. Before enabling CFM processing on the switch, first configure the required CFM domains, maintenance associations, and static MEPs. Then set the delay time to wait for a remote MEP comes up before the switch starts cross-checking the end points learned through CCMs against those stored in the static list.
4. Adjust the parameters for the link trace cache as required.
5. Enable the required traps for continuity check and cross-check errors. Remember that the "Connectivity Check" and "Cross Check" fields on the MA Configuration page must be enabled before related errors can be generated.
6. Click Apply.

Figure 293: Configuring Global Settings for CFM

The screenshot shows the 'Administration > CFM' web interface. At the top, there is a 'Step:' dropdown menu set to '1. Configure Global'. Below this, the 'Global Configuration' section contains the following settings:

Setting	Value
CFM Status	<input checked="" type="checkbox"/> Enabled
MEP Cross Check Start Delay (1-65535)	10 sec
Link Trace Cache	<input checked="" type="checkbox"/> Enabled
Link Trace Cache Hold Time (1-65535)	100 min
Link Trace Cache Size (1-4095)	100 entries

Below the Global Configuration section is the 'SNMP Trap Configuration' section, which contains the following settings:

Setting	Value
Connectivity Check Config	<input type="checkbox"/> Enabled
Connectivity Check Loop	<input type="checkbox"/> Enabled
Connectivity Check MEP Down	<input type="checkbox"/> Enabled
Connectivity Check MEP Up	<input type="checkbox"/> Enabled
Cross Check MA Up	<input type="checkbox"/> Enabled
Cross Check MEP Missing	<input type="checkbox"/> Enabled
Cross Check MEP Unknown	<input type="checkbox"/> Enabled

At the bottom right of the interface are two buttons: 'Apply' and 'Revert'.

CONFIGURING INTERFACES FOR CFM

CFM processes are enabled by default for all physical interfaces, both ports and trunks. You can use the Administration > CFM (Configure Interface) page to change these settings.

CLI REFERENCES

- ◆ "ethernet cfm port-enable" on page 1307

COMMAND USAGE

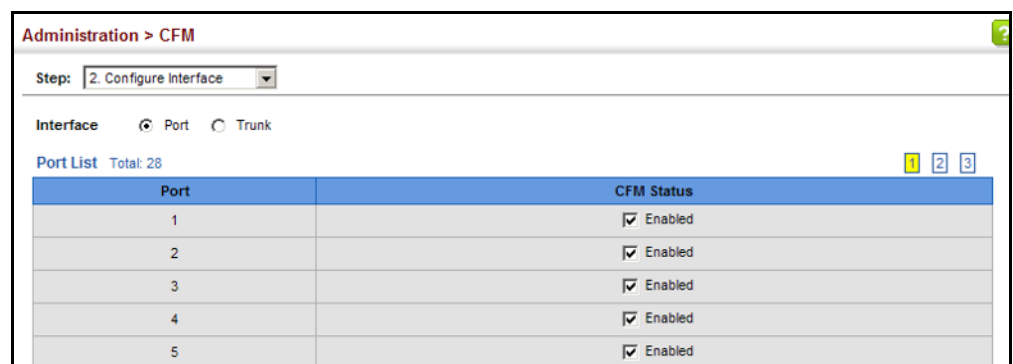
- ◆ An interface must be enabled before a MEP can be created (see "Configuring Maintenance End Points").
- ◆ If a MEP has been configured on an interface, it must first be deleted before CFM can be disabled on that interface.
- ◆ When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

WEB INTERFACE

To enable CFM on an interface:

1. Click Administration, CFM.
2. Select Configure Interface from the Step list.
3. Select Port or Trunk.
4. Enable CFM on the required interface.
5. Click Apply.

Figure 294: Configuring Interfaces for CFM



Administration > CFM

Step: 2. Configure Interface

Interface: ☒ Port ☐ Trunk

Port List Total: 28

Port	CFM Status
1	<input checked="" type="checkbox"/> Enabled
2	<input checked="" type="checkbox"/> Enabled
3	<input checked="" type="checkbox"/> Enabled
4	<input checked="" type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled

CONFIGURING CFM MAINTENANCE DOMAINS

Use the Administration > CFM (Configure MD) pages to create and configure a Maintenance Domain (MD) which defines a portion of the network for which connectivity faults can be managed. Domain access points are set up on the boundary of a domain to provide end-to-end connectivity fault detection, analysis, and recovery. Domains can be configured in a hierarchy to provide management access to the same basic network resources for different user levels.

CLI REFERENCES

- ◆ ["CFM Commands" on page 1295](#)

COMMAND USAGE

Configuring General Settings

- ◆ 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 (see ["Configuring Maintenance End Points"](#)) or MAs (see ["Configuring CFM Maintenance Associations"](#)) are configured for a domain, 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 (see ["Configuring Maintenance End Points"](#)).

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 Type 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 for an MA (see "[Configuring CFM Maintenance Associations](#)") takes precedence over the method defined on the CFM Domain List.

Configuring Fault Notification

- ◆ A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that the configured time period (MEP Fault Notify Alarm Time) has passed with one or more defects indicated, and fault alarms are enabled at or above the specified priority level (MEP Fault Notify Lowest Priority). The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (MEP Fault Notify Reset Time) 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 levels include the following options:

Table 33: 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 34: MEP Defect Descriptions

Defect	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.

PARAMETERS

These parameters are displayed:

Creating a Maintenance Domain

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MD Name** – Maintenance domain name. (Range: 1-43 alphanumeric characters)
- ◆ **MD Level** – Authorized maintenance level for this domain. (Range: 0-7)
- ◆ **MIP Creation 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.

Configuring Detailed Settings for a Maintenance Domain

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MEP Archive Hold Time** – The time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. (Range: 1-65535 minutes; Default: 100 minutes)

A change to the hold time only applies to entries stored in the database after this attribute is changed.
- ◆ **MEP Fault Notify Lowest Priority** – The lowest priority defect that is allowed to generate a fault alarm. (Range: 1-6, Default: 2)
- ◆ **MEP Fault Notify Alarm Time** – The time that one or more defects must be present before a fault alarm is issued. (Range: 3-10 seconds; Default: 3 seconds)
- ◆ **MEP Fault Notify Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. (Range: 3-10 seconds; Default: 10 seconds)

WEB INTERFACE

To create a maintenance domain:

1. Click Administration, CFM.
2. Select Configure MD from the Step list.
3. Select Add from the Action list.
4. Specify the maintenance domains and authorized maintenance levels (thereby setting the hierarchical relationship with other domains).
5. Specify the manner in which MIPs can be created within each domain.
6. Click Apply.

Figure 295: Configuring Maintenance Domains

Administration > CFM

Step: 1. Configure MD Action: Add

MD Index (1-65535) 1

MD Name voip

MD Level (0-7) 3

MIP Creation Type Explicit

Apply Revert

To show the configured maintenance domains:

1. Click Administration, CFM.
2. Select Configure MD from the Step list.
3. Select Show from the Action list.

Figure 296: Showing Maintenance Domains

Administration > CFM

Step: 1. Configure MD Action: Show

CFM MD List Total: 1

	MD Index	MD Name	MD Level	MIP Creation Type
<input type="checkbox"/>	1	voip	3	Explicit

Delete Revert

To configure detailed settings for maintenance domains:

1. Click Administration, CFM.
2. Select Configure MD from the Step list.
3. Select Configure Details from the Action list.
4. Select an entry from the MD Index.
5. Specify the MEP archive hold and MEP fault notification parameters.
6. Click Apply

Figure 297: Configuring Detailed Settings for Maintenance Domains

The screenshot shows a web interface for configuring maintenance domains. At the top, it says 'Administration > CFM'. Below that, there are two dropdown menus: 'Step: 3. Configure MD' and 'Action: Configure Details'. The main section is titled 'MD Index' and contains a table with five rows of configuration parameters:

Parameter	Value
MD Index	1
MEP Archive Hold Time (1-65535)	100
MEP Fault Notify Lowest Priority (1-6)	2
MEP Fault Notify Alarm Time (3-10)	3
MEP Fault Notify Reset Time (3-10)	10

At the bottom right of the form, there are two buttons: 'Apply' and 'Revert'.

CONFIGURING CFM MAINTENANCE ASSOCIATIONS

Use the Administration > CFM (Configure MA) pages to create and configure the Maintenance Associations (MA) which define a unique CFM service instance. Each MA can be identified by its parent MD, the MD's maintenance level, the VLAN assigned to the MA, and the set of maintenance end points (MEPs) assigned to it.

CLI REFERENCES

- ◆ ["CFM Commands" on page 1295](#)

COMMAND USAGE

Creating a Maintenance Association

- ◆ Use the Configure MA – Add screen to create an MA within the selected MD, map it to a customer service instance (S-VLAN), and set the manner in which MIPs are created for this service instance. Then use the MEP List to assign domain service access points (DSAPs) to this service instance (see ["Configuring Maintenance End Points" on page 527](#)).
- ◆ An MA must be defined before any associated DSAPs or remote MEPs can be assigned (see ["Configuring Remote Maintenance End Points" on page 528](#)).

- ◆ Multiple domains at the same maintenance level cannot have an MA on the same VLAN (see ["Configuring CFM Maintenance Domains" on page 517](#)).
- ◆ Before removing an MA, first remove the MEPs assigned to it (see ["Configuring Maintenance End Points" on page 527](#)).
- ◆ For a detailed description of the MIP types, refer to the Command Usage section under ["Configuring CFM Maintenance Domains" on page 517](#).

Configuring Detailed Settings for a Maintenance Association

- ◆ 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 MEP ID, 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).
- ◆ The interval at which CCMs are issued should 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.

PARAMETERS

These parameters are displayed:

Creating a Maintenance Association

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MA Name** – MA name. (Range: 1-43 alphanumeric characters)
Each MA name must be unique within the CFM domain.
- ◆ **Primary VLAN** – Service VLAN ID. (Range: 1-4093)
This is the VLAN through which all CFM functions are executed for this MA.

- ◆ **MIP Creation 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 for 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.

Configuring Detailed Settings for a Maintenance Association

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MA Name Format** – 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.
 - **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.
- ◆ **Interval Level** – The delay between sending CCMs. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (Options: 4 - 1 second, 5 - 10 seconds, 6 - 1 minute, 7 - 10 minutes)
- ◆ **Connectivity Check** – Enables transmission of CCMs. (Default: Disabled)
- ◆ **Cross Check** – Enables cross-checking between a static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through CCMs.

Before starting the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the Remote MEP List (see "[Configuring Remote Maintenance End Points](#)"). These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.

The cross-check start delay, which sets the maximum delay this device waits for a remote MEP to come up before starting the cross-check operation, is a domain-level parameter. To set this parameter, use the CFM MD Configuration screen (see "[Configuring CFM Maintenance Domains](#)").

- ◆ **AIS Status** – Enables/disables suppression of the Alarm Indication Signal (AIS). (Default: Disabled)
- ◆ **AIS Period** – Configures the period at which AIS is sent in an MA. (Range: 1 or 60 seconds; Default: 1 second)

- ◆ **AIS Transmit Level** – Configure the AIS maintenance level in an MA.
(Range: 0-7; Default is 0)
AIS Level must follow this rule: AIS Level \geq Domain Level
- ◆ **AIS Suppress Alarm** – Enables/disables suppression of the AIS.
(Default: Disabled)

WEB INTERFACE

To create a maintenance association:

1. Click Administration, CFM.
2. Select Configure MA from the Step list.
3. Select Add from the Action list.
4. Select an entry from the MD Index list.
5. Specify the MAs assigned to each domain, the VLAN through which CFM messages are passed, and the manner in which MIPs can be created within each MA.
6. Click Apply.

Figure 298: Creating Maintenance Associations

Administration > CFM

Step: 2. Configure MA Action: Add

MD Index 1

MA Index (1-2147483647) 1

MA Name rd

Primary VLAN (1-4093) 1

MIP Creation Type Default

Apply Revert

To show the configured maintenance associations:

1. Click Administration, CFM.
2. Select Configure MA from the Step list.
3. Select Show from the Action list.
4. Select an entry from the MD Index list.

Figure 299: Showing Maintenance Associations

Administration > CFM

Step: 4. Configure MA Action: Show

MD Index 1

CFM MA List Total: 1

	MA Index	MA Name	Primary VLAN	MIP Creation Type
<input type="checkbox"/>	1	rd	1	Default

Delete Revert

To configure detailed settings for maintenance associations:

1. Click Administration, CFM.
2. Select Configure MA from the Step list.
3. Select Configure Details from the Action list.
4. Select an entry from MD Index and MA Index.
5. Specify the CCM interval, enable the transmission of connectivity check and cross check messages, and configure the required AIS parameters.
6. Click Apply

Figure 300: Configuring Detailed Settings for Maintenance Associations

Administration > CFM

Step: 4. Configure MA Action: Configure Details

MD Index 1

MA Index 1

MA Name Format Character String

Interval Level (4-7) 4

Connectivity Check ☒ Enabled

Cross Check ☒ Enabled

AIS Status ☒ Enabled

AIS Period 1

AIS Transmit Level (0-7) 0

AIS Suppress Alarm ☐ Enabled

Apply Revert

CONFIGURING MAINTENANCE END POINTS

Use the Administration > CFM (Configure MEP – Add) page to configure Maintenance End Points (MEPs). MEPs, also called Domain Service Access Points (DSAPs), must be configured at the domain boundary to provide management access for each maintenance association.

CLI REFERENCES

- ◆ ["CFM Commands" on page 1295](#)

COMMAND USAGE

- ◆ CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured (see ["Configuring CFM Maintenance Domains"](#)), (2) maintenance association within the domain (see ["Configuring CFM Maintenance Associations"](#)), and (3) finally the MEPs using the MEP List.
- ◆ An interface may belong to more than one domain, or to 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.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **MEP Direction** – 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** option is not selected, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
- ◆ **Interface** – Indicates a port or trunk.

WEB INTERFACE

To configure a maintenance end point:

1. Click Administration, CFM.
2. Select Configure MEP from the Step list.
3. Select Add from the Action list.
4. Select an entry from MD Index and MA Index.
5. Specify the MEPs assigned to each MA, set the MEP identifier, the direction in which the MEP faces, and the physical interface serving as the DSAP.

6. Click Apply.

Figure 301: Configuring Maintenance End Points

Administration > CFM

Step: 3. Configure MEP Action: Add

MD Index 1

MA Index 1

MEP ID (1-8191) 1

MEP Direction ☐ Up

Interface ☒ Port 1 ☐ Trunk

Apply Revert

To show the configured maintenance end points:

1. Click Administration, CFM.
2. Select Configure MEP from the Step list.
3. Select Show from the Action list.
4. Select an entry from MD Index and MA Index.

Figure 302: Showing Maintenance End Points

Administration > CFM

Step: 3. Configure MEP Action: Show

MD Index 1

MA Index 1

CFM Maintenance Association End Point List Total: 1

	MEP ID	MEP Direction	Interface
<input type="checkbox"/>	1	Down	Unit 1 / Port 1

Delete Revert

CONFIGURING REMOTE MAINTENANCE END POINTS

Use the Administration > CFM (Configure Remote MEP – Add) page to specify remote maintenance end points (MEPs) set on other CFM-enabled devices within a common MA. Remote MEPs can be added to a static list in this manner to verify that each entry has been properly configured and is operational. When cross-checking is enabled, the list of statically configured remote MEPs is compared against the MEPs learned through continuity check messages (CCMs), and any discrepancies reported via SNMP traps.

CLI REFERENCES

- ◆ "CFM Commands" on page 1295

COMMAND USAGE

- ◆ All MEPs that exist on other devices inside a maintenance association should be statically configured to ensure full connectivity through the cross-check process.
- ◆ Remote MEPs can only be configured if local domain service access points (DSAPs) have already been created (see ["Configuring Maintenance End Points"](#)) 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.
- ◆ The MEP cross-check start delay which sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation can be configured on the Configure Global page (see ["Configuring Global Settings for CFM"](#)).
- ◆ SNMP traps for continuity check events discovered by cross-check operations can also be configured on the Configure Global page (see ["Configuring Global Settings for CFM"](#)).

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

WEB INTERFACE

To configure a remote maintenance end point:

1. Click Administration, CFM.
2. Select Configure Remote MEP from the Step list.
3. Select Add from the Action list.
4. Select an entry from MD Index and MA Index.
5. Specify the remote MEPs which exist on other devices within the same MA.
6. Click Apply.

Figure 303: Configuring Remote Maintenance End Points

Administration > CFM

Step: 4. Configure Remote MEP Action: Add

MD Index 1

MA Index 1

MEP ID (1-8191) 2

Apply Revert

To show the configured remote maintenance end points:

1. Click Administration, CFM.
2. Select Configure MEP from the Step list.
3. Select Show from the Action list.
4. Select an entry from MD Index and MA Index.

Figure 304: Showing Remote Maintenance End Points

Administration > CFM

Step: 4. Configure Remote MEP Action: Show

MD Index 1

MA Index 1

CFM Remote Maintenance Association End Point List Total: 1

	MEP ID
<input type="checkbox"/>	2

Delete Revert

TRANSMITTING LINK
TRACE MESSAGES

Use the Administration > CFM (Transmit Link Trace) page to transmit link trace messages (LTMs). These messages can isolate connectivity faults by tracing the path through a network to the designated target node (i.e., a remote maintenance end point).

CLI REFERENCES

- ◆ "CFM Commands" on page 1295

COMMAND USAGE

- ◆ LTMs 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 (see "Configuring Remote Maintenance End Points").
- ◆ If MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the Show Remote MEP page (see "Displaying Remote MEPs") to verify that a MAC address has been learned for the target MEP.

- ◆ LTM's 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.
- ◆ LTM's 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.
- ◆ Parameters controlling the link trace cache, including operational state, entry hold time, and maximum size can be configured on the Configure Global page (see "[Configuring Global Settings for CFM](#)").

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a link trace message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- ◆ **TTL** – The time to live of the link trace message. (Range: 0-255 hops)

WEB INTERFACE

To transmit link trace messages:

1. Click Administration, CFM.
2. Select Transmit Link Trace from the Step list.
3. Select an entry from MD Index and MA Index.
4. Specify the source MEP, the target MEP using either its MEP identifier or MAC address, and set the maximum number of hops allowed in the TTL field.

- 5. Click Apply.
- 6. Check the results in the Link Trace cache (see ["Displaying the Link Trace Cache"](#)).

Figure 305: Transmitting Link Trace Messages

The screenshot shows a web interface for 'Administration > CFM'. The 'Step' dropdown is set to '7. Transmit Link Trace'. The form contains the following fields:

- MD Index: 1
- MA Index: 1
- Source MEP ID (1-8191): 1
- Target: ☒ MEP ID (1-8191) 2
- ☐ MAC Address
- TTL (0-255): 5

At the bottom right, there are 'Apply' and 'Revert' buttons.

**TRANSMITTING LOOP
BACK MESSAGES**

Use the Administration > CFM (Transmit Loopback) page to transmit Loopback Messages (LBMs). These messages can be used to isolate or verify connectivity faults by submitting a request to a target node (i.e., a remote MEP or MIP) to echo the message back to the source.

CLI REFERENCES

- ◆ ["CFM Commands" on page 1295](#)

COMMAND USAGE

- ◆ Loopback 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.
- ◆ The point from which the loopback message is transmitted (i.e., a local DSAP) and the target maintenance point must be within the same MA.
- ◆ If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.
- ◆ 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.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)

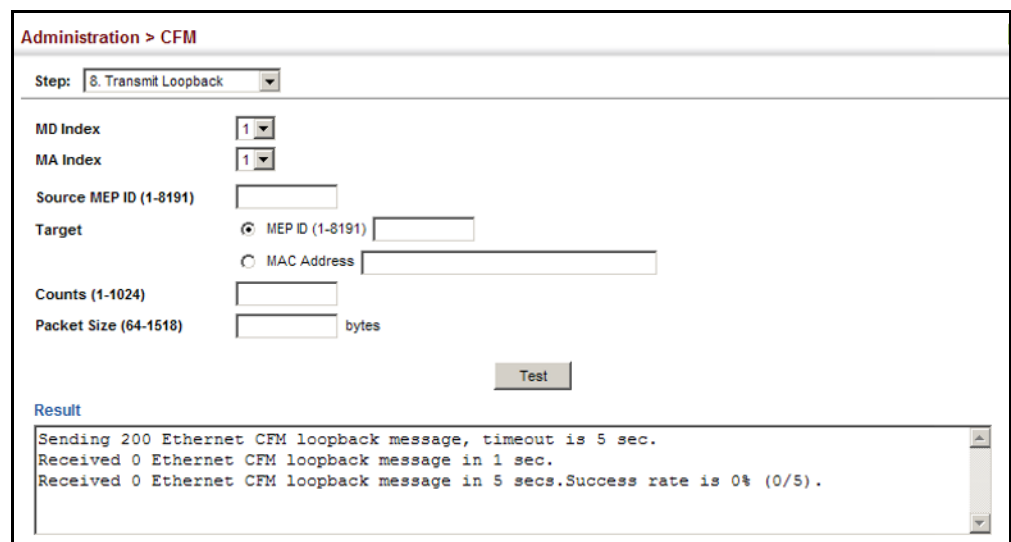
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a loopback message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- ◆ **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: 64 bytes)

WEB INTERFACE

To transmit loopback messages:

1. Click Administration, CFM.
2. Select Transmit Loopback from the Step list.
3. Select an entry from MD Index and MA Index.
4. Specify the source MEP, the target MEP using either its MEP identifier or MAC address, set the number of times the loopback message is to be sent.
5. Click Apply.

Figure 306: Transmitting Loopback Messages



Administration > CFM

Step: 8. Transmit Loopback

MD Index: 1

MA Index: 1

Source MEP ID (1-8191):

Target:

☒ MEP ID (1-8191)

☐ MAC Address

Counts (1-1024):

Packet Size (64-1518): bytes

Test

Result

```

Sending 200 Ethernet CFM loopback message, timeout is 5 sec.
Received 0 Ethernet CFM loopback message in 1 sec.
Received 0 Ethernet CFM loopback message in 5 secs. Success rate is 0% (0/5).
  
```

TRANSMITTING DELAY-MEASURE REQUESTS Use the Administration > CFM (Transmit Delay Measure) page to send periodic delay-measure requests to a specified MEP within a maintenance association.

CLI REFERENCES

- ◆ ["ethernet cfm delay-measure two-way" on page 1334](#)

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 function.
- ◆ 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 TxTimestampb (Timestamp at the time of transmitting a frame with DM reply information):
$$\text{Frame Delay} = (\text{RxTimeStampb} - \text{TxTimeStampf}) - (\text{TxTimestampb} - \text{RxTimeStampf})$$
- ◆ 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.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a delay-measure message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

- ◆ **Count** – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5; Default: 5)
- ◆ **Packet Size** – The size of the delay-measure message. (Range: 64-1518 bytes; Default: 64 bytes)
- ◆ **Interval** – The transmission delay between delay-measure messages. (Range: 1-5 seconds; Default: 1 second)
- ◆ **Timeout** – The timeout to wait for a response. (Range: 1-5 seconds; Default: 5 seconds)

WEB INTERFACE

To transmit delay-measure messages:

1. Click Administration, CFM.
2. Select Transmit Delay Measure from the Step list.
3. Select an entry from MD Index and MA Index.
4. Specify the source MEP, the target MEP using either its MEP identifier or MAC address, set the number of times the delay-measure message is to be sent, the interval, and the timeout.
5. Click Apply.

Figure 307: Transmitting Delay-Measure Messages

Administration > CFM

Step: 7. Transmit Delay Measure

MD Index: 1

MA Index: 3

Source MEP ID (1-8191):

Target: ☒ MEP ID (1-8191) ☐ MAC Address

Counts (1-5):

Packet Size (64-1518): bytes

Interval (1-5): ms

Timeout (1-5): ms

Apply
Revert

Result

Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.

Sequence	Delay Time (ms.)	Delay Variation (ms.)
1	< 10	0
2	10	10
3	< 10	10
4	< 10	0
5	< 10	0

Success rate is 100% (5/5), delay time min/avg/max=0/2/10 ms.
Average frame delay variation is 4 ms.

DISPLAYING LOCAL MEPS Use the Administration > CFM > Show Information (Show Local MEP) page to show information for the MEPs configured on this device.

CLI REFERENCES

- ◆ "show ethernet cfm maintenance-points local" on page 1311

PARAMETERS

These parameters are displayed:

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MD Name** – Maintenance domain name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **Direction** – Direction in which the MEP communicates CFM messages:
 - Down indicates that the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
 - 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.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Interface** – Physical interface of this entry (either a port or trunk).
- ◆ **CC Status** – Shows administrative status of CCMs.
- ◆ **MAC Address** – MAC address of this MEP entry.

WEB INTERFACE

To show information for the MEPs configured on this device:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Local MEP from the Action list.

Figure 308: Showing Information on Local MEPs

Administration > CFM

Step: 7. Show Information

Action: Show Local MEP

CFM Local Maintenance Association End Point Information Total: 1

MEP ID	MD Name	Level	Direction	Primary VLAN	Interface	CC Status	MAC Address
1	voip	3	Down	1	Eth 1/1	Enabled	00-E0-0C-00-00-FE

DISPLAYING DETAILS FOR LOCAL MEPS Use the Administration > CFM > Show Information (Show Local MEP Details) page to show detailed CFM information about a local MEP in the continuity check database.

CLI REFERENCES

- ◆ ["show ethernet cfm maintenance-points local detail mep" on page 1312](#)

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **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.

WEB INTERFACE

To show detailed information for the MEPs configured on this device:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Local MEP Details from the Action list.
4. Select an entry from MD Index and MA Index.
5. Select a MEP ID.

Figure 309: Showing Detailed Information on Local MEPs

Administration > CFM

Step: 10. Show Information Action: Show Local MEP Details

MD Index: 1
MA Index: 1
MEP ID: 1

Query

MD Name	md1
MA Name	ma1
MA Name Format	Character String
Level	0
Direction	Up
Interface	Unit 1 / Port 2
CC Status	Enabled
MAC Address	00-1B-D5-50-91-FD
Defect Condition	No Defect
Received RDI	False
AIS Status	Enabled
AIS Period	60 sec
AIS Transmit Level	Default
Suppress Alarm	Enabled
Suppressing Alarms	Disabled

DISPLAYING LOCAL MIPs Use the Administration > CFM > Show Information (Show Local MIP) page to show the MIPs on this device discovered by the CFM protocol. (For a description of MIPs, refer to the Command Usage section under "Configuring CFM Maintenance Domains".)

CLI REFERENCES

◆ "show ethernet cfm maintenance-points local" on page 1311

PARAMETERS

These parameters are displayed:

- ◆ **MD Name** – Maintenance domain name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Interface** – Physical interface of this entry (either a port or trunk).

WEB INTERFACE

To show information for the MIPs discovered by the CFM protocol:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Local MIP from the Action list.

Figure 310: Showing Information on Local MIPs

Administration > CFM				
Step:	10. Show Information	Action:	Show Local MIP	
CFM Local Maintenance Association Intermediate Point Information Total: 27				
MD Name	Level	MA Name	Primary VLAN	Interface
voip	3	rd	1	Unit 1 / Port 2
voip	3	rd	1	Unit 1 / Port 3
voip	3	rd	1	Unit 1 / Port 4
voip	3	rd	1	Unit 1 / Port 5
voip	3	rd	1	Unit 1 / Port 6
voip	3	rd	1	Unit 1 / Port 7
voip	3	rd	1	Unit 1 / Port 8
voip	3	rd	1	Unit 1 / Port 9
voip	3	rd	1	Unit 1 / Port 10

DISPLAYING REMOTE MEPS Use the Administration > CFM > Show Information (Show Remote MEP) page to show MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

CLI REFERENCES

- ◆ "show ethernet cfm maintenance-points remote detail" on page 1313
- ◆ "clear ethernet cfm maintenance-points remote" on page 1318

PARAMETERS

These parameters are displayed:

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **MEP Up** – Indicates whether or not this MEP is functioning normally.
- ◆ **Remote 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.)

WEB INTERFACE

To show information for remote MEPs:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Remote MEP from the Action list.

Figure 311: Showing Information on Remote MEPs

Administration > CFM

Step: 10. Show Information Action: Show Remote MEP

CFM Remote Maintenance Association End Point Information Total: 1

MEP ID	MA Name	Level	Primary VLAN	MEP Up	Remote MAC Address
1	ma1	0	2	Yes	00-01-02-03-04-05

Clear

DISPLAYING DETAILS FOR REMOTE MEPS

Use the Administration > CFM > Show Information (Show Remote MEP Details) page to show detailed information for MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

CLI REFERENCES

- ◆ ["show ethernet cfm maintenance-points remote detail" on page 1313](#)

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **MD Name** – Maintenance domain name.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **MAC Address** – MAC address of this MEP entry.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **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** – The number of CCM packets received successfully and those with errors.
- ◆ **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.

WEB INTERFACE

To show detailed information for remote MEPs:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Remote MEP Details from the Action list.
4. Select an entry from MD Index and MA Index.
5. Select a MEP ID.

Figure 312: Showing Detailed Information on Remote MEPs

Administration > CFM	
Step:	10. Show Information
Action:	Show Remote MEP Details
MD Index	1
MA Index	1
MEP ID	1
Query	
MD Name	md1
MA Name	ma1
Level	0
MAC Address	00-1B-D5-50-91-FD
Primary VLAN	2
Incoming Port	Unit 1 / Port 2
CC Lifetime	75 sec
Age of Last CC Message	60 sec
Frame Loss	0
CC Packet Statistics	139 / 0 (Received / Error)
Port State	Enabled
Interface State	Enabled
Crosscheck Status	Disabled

DISPLAYING THE LINK TRACE CACHE Use the Administration > CFM > Show Information (Show Link Trace Cache) page to show information about link trace operations launched from this device.

CLI REFERENCES

- ◆ "show ethernet cfm linktrace-cache" on page 1328
- ◆ "clear ethernet cfm linktrace-cache" on page 1328

PARAMETERS

These parameters are displayed:

- ◆ **Hops** – The number hops taken to reach the target MEP.
- ◆ **MA** – Maintenance association name.
- ◆ **IP/Alias Address** – IP address or DNS 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 Address** – MAC address of the ingress port on the target device.
- ◆ **Egress MAC Address** – MAC address of the egress port on the target device.
- ◆ **Ingress 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.
- ◆ **Egress 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.

◆ **Reply** – Reply action:

- FDB – Target address found in forwarding database.
- MPDB – Target address found in the maintenance point database.
- HIT – Target located on this device.

WEB INTERFACE

To show information about link trace operations launched from this device:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Link Trace Cache from the Action list.

Figure 313: Showing the Link Trace Cache

Hops	MA	IP/Alias Address	Forwarded	Ingress MAC Address	Egress MAC Address	Ingress Action	Egress Action	Reply
1	denver	11-11-11-11-11-11	Forwarded	11-11-11-11-11-12	11-11-11-11-11-13	OK	OK	FDB
2	boston	AA-BB-CC-00-04-00	Not Forwarded					

**DISPLAYING FAULT
NOTIFICATION
SETTINGS**

Use the Administration > CFM > Show Information (Show Fault Notification Generator) page to display configuration settings for the fault notification generator.

CLI REFERENCES

- ◆ ["show ethernet cfm fault-notify-generator" on page 1333](#)

PARAMETERS

These parameters are displayed:

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MD Name** – Maintenance domain name.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Highest 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 alarm²².

- ◆ **Alarm Time** – The time a defect must exist before a fault alarm is issued²².
- ◆ **Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued²².

WEB INTERFACE

To show configuration settings for the fault notification generator:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Fault Notification Generator from the Action list.

Figure 314: Showing Settings for the Fault Notification Generator

CFM Fault Notification Generator Information Total: 1						
MEP ID	MD Name	MA Name	Highest Defect	Lowest Alarm	Alarm Time (sec)	Reset Time (sec)
1	aa	bb	NONE	allDef	3	3

DISPLAYING CONTINUITY CHECK ERRORS

Use the Administration > CFM > Show Information (Show Continuity Check Error) page to display the CFM continuity check errors logged on this device.

CLI REFERENCES

- ◆ ["show ethernet cfm errors" on page 1320](#)
- ◆ ["clear ethernet cfm errors" on page 1319](#)

PARAMETERS

These parameters are displayed:

- ◆ **Level** – Maintenance level associated with this entry.
- ◆ **Primary VLAN** – VLAN in which this error occurred.
- ◆ **MEP ID** – Identifier of remote MEP.
- ◆ **Interface** – Port at which the error was recorded.
- ◆ **Remote MAC** – MAC address of remote MEP.
- ◆ **Reason** – Error types include:
 - LEAK – MA x is associated with a specific VID list²³, 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,

²². See ["Configuring CFM Maintenance Domains" on page 517](#).

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.

- VIDS – MA x is associated with a specific VID list²³, an MEP is configured facing inward (up) 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.
- EXCESS_LEV – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.
- 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.

◆ **MA Name** – The maintenance association for this entry.

WEB INTERFACE

To show CFM continuity check errors:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Continuity Check Error from the Action list.

Figure 315: Showing Continuity Check Errors

Administration > CFM						
Step: 10. Show Information Action: Show Continuity Check Error						
CFM Continuity Check Error Information Total: 1						
Level	Primary VLAN	MEP ID	Interface	Remote MAC	Reason	MA Name
5	2	40	Unit 1 / Port 10	00-01-02-03-04-05	LEAK	aa

Clear

23. 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.

OAM CONFIGURATION

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, loopback testing, and displaying remote device information.

ENABLING OAM ON LOCAL PORTS

Use the Administration > OAM > Interface page to enable OAM functionality on the selected port. Not all CPEs support operation and maintenance functions, so OAM is therefore disabled by default. If a CPE supports OAM, this functionality must first be enabled on the connected port to gain access to the configuration functions provided under the OAM menu.

CLI REFERENCES

- ◆ ["OAM Commands" on page 1337](#)

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Admin Status** – Enables or disables OAM functions. (Default: Disabled)
- ◆ **Operation State** – Shows the operational state between the local and remote OAM devices. This value is always "disabled" if OAM is disabled on the local interface.

Table 35: OAM Operation State

State	Description
Disabled	OAM is disabled on this interface via the OAM Admin Status.
Link Fault	The link has detected a fault or the interface is not operational.
Passive Wait	This value is returned only by OAM entities in passive mode and indicates the OAM entity is waiting to see if the peer device is OAM capable.
Active Send Local	This value is used by active mode devices and indicates the OAM entity is actively trying to discover whether the peer has OAM capability but has not yet made that determination.
Send Local And Remote	The local OAM entity has discovered the peer but has not yet accepted or rejected the configuration of the peer.
Send Local And Remote OK	OAM peering is allowed by the local device.
OAM Peering Locally Rejected	The local OAM entity rejects the peering.
OAM Peering Remotely Rejected	The remote OAM entity rejects the peering.

Table 35: OAM Operation State (Continued)

State	Description
Operational	When the local OAM entity learns that both it and the remote OAM entity have accepted the peering, the state moves to this state.
Non Oper Half Duplex	This state is returned whenever Ethernet OAM is enabled but the interface is in half-duplex operation.

- ◆ **Mode** – Sets the OAM operation mode. (Default: Active)
 - **Active** – All OAM functions are enabled.
 - **Passive** – All OAM functions are enabled, except for OAM discovery, sending variable request OAMPDUs, and sending loopback control OAMPDUs.
- ◆ **Critical Link Event** – Controls reporting of critical link events to its OAM peer.
 - **Dying Gasp** – If an unrecoverable condition occurs, the local OAM entity (i.e., this switch) indicates this by immediately sending a trap message. (Default: Enabled)

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.

- **Critical Event** – If a critical event occurs, the local OAM entity 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. (Default: Enabled)

Critical events 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.
- ◆ **Errored Frame** – Controls reporting of errored frame link events.

An errored frame is a frame in which one or more bits are errored.

An errored frame link event occurs if the threshold is reached or exceeded within the specified period.

If reporting is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU to the remote OAM entity. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

 - **Status** – Enables reporting of errored frame link events. (Default: Enabled)

- **Window Size** – The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 in units of 10 milliseconds; Default: 10 units of 10 milliseconds, or the equivalent of 1 second)
- **Threshold Count** – The threshold for errored frame link events. (Range: 1-65535; Default: 1)

WEB INTERFACE

To enable OAM functionality on the selected port:

1. Click Administration, OAM, Interface.
2. Set the OAM administrative status and operational mode for the required ports. Specify whether or not critical link events will be reported by the switch. Specify whether errored frame link events will be reported, as well as the required window size and threshold.
3. Click Apply.

Figure 316: Enabling OAM for Local Ports

Administration > OAM > Interface

OAM Port List Total: 28

Port	Admin Status	Operation State	Mode	Critical Link Event		Errored Frame		
				Dying Gasp	Critical Event	Status	Window Size (10-65535 1/10 sec)	Threshold Count (1-65535)
1	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
2	<input checked="" type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
3	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
4	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
5	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
6	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
7	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
8	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
9	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
10	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1

Apply Revert

DISPLAYING STATISTICS FOR OAM MESSAGES

Use the Administration > OAM > Counters page to display statistics for the various types of OAM messages passed across each port.

CLI REFERENCES

- ◆ "show efm oam counters interface" on page 1344

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Clear** – Clears statistical counters for the selected ports.

- ◆ **OAMPDU** – Message types transmitted and received by the OAM protocol, including Information OAMPDUs, unique Event OAMPDUs, Loopback Control OAMPDUs, and Organization Specific OAMPDUs.

WEB INTERFACE

To display statistics for OAM messages:

1. Click Administration, OAM, Counters.

Figure 317: Displaying Statistics for OAM Messages

Administration > OAM > Counters

OAM Port Counters Total: 28

	Port	OAMPDU							
		Information		Event Notification		Loopback Control		Organization Specific	
		Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
<input type="checkbox"/>	1	3	0	0	0	0	0	0	0
<input type="checkbox"/>	2	0	0	0	0	0	0	0	0
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	0	0	0	0	0	0	0	0
<input type="checkbox"/>	7	0	0	0	0	0	0	0	0
<input type="checkbox"/>	8	0	0	0	0	0	0	0	0
<input type="checkbox"/>	9	0	0	0	0	0	0	0	0
<input type="checkbox"/>	10	0	0	0	0	0	0	0	0

Clear

DISPLAYING THE OAM EVENT LOG

Use the Administration > OAM > Event Log page to display link events for the selected port.

CLI REFERENCES

- ◆ ["show efm oam event-log interface" on page 1344](#)

COMMAND USAGE

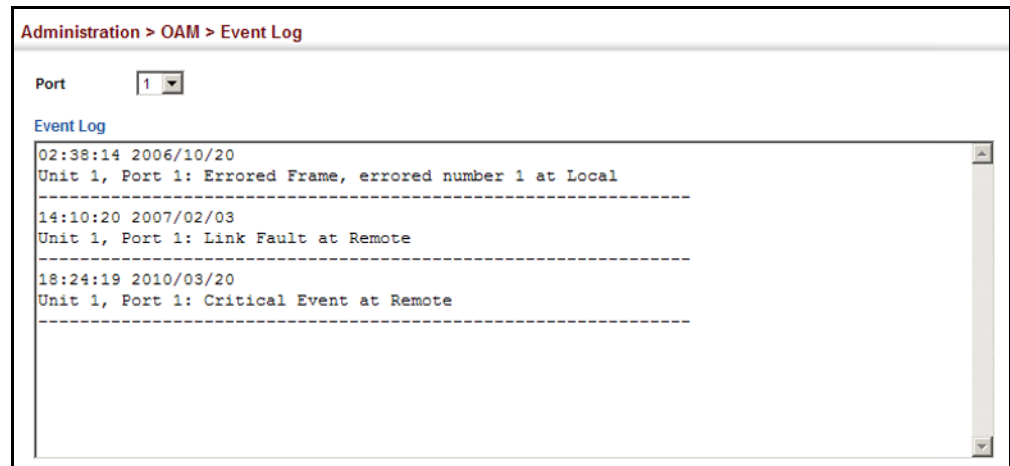
- ◆ When a link event occurs, no matter whether the location is local or remote, this information is entered in OAM event log.
- ◆ When the log system becomes full, older events are automatically deleted to make room for new entries.
- ◆ The time of locally generated events can be accurately retrieved from the sysUpTime variable. For remotely generated events, the time of an event is indicated by the reception of an Event Notification OAMPDU from the peer.

WEB INTERFACE

To display link events for the selected port:

1. Click Administration, OAM, Event Log.
2. Select a port from the drop-down list.

Figure 318: Displaying the OAM Event Log



DISPLAYING THE STATUS OF REMOTE INTERFACES

Use the Administration > OAM > Remote Interface page to display information about attached OAM-enabled devices.

CLI REFERENCES

- ◆ ["show efm oam status remote interface" on page 1346](#)

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **MAC Address** – MAC address of the OAM peer.
- ◆ **OUI** – Organizational Unit Identifier of the OAM peer.
- ◆ **Remote Loopback** – Shows if remote loopback is supported by the OAM peer.
- ◆ **Unidirectional Function** – Shows if this function is supported by the OAM peer.

If supported, this indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (where traffic flows in one direction only). Some newer physical layer devices support the optional ability to encode and transmit data while one direction of the link is non-operational. This function allows OAM remote fault indication during fault conditions. This switch does

not support the unidirectional function, but can parse error messages sent from a peer with unidirectional capability.

- ◆ **Link Monitor** – Shows if the OAM entity can send and receive Event Notification OAMPDUs.
- ◆ **MIB Variable Retrieval** – Shows if the OAM entity can send and receive Variable Request and Response OAMPDUs.

WEB INTERFACE

To display information about attached OAM-enabled devices:

1. Click Administration, OAM, Remote Interface.

Figure 319: Displaying Status of Remote Interfaces

Administration > OAM > Remote Interface

OAM Remote Port List Total: 28

Port	MAC Address	OUI	Remote Loopback	Unidirectional Function	Link Monitor	MIB Variable Retrieval
1	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
2	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
3	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
4	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
5	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
6	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
7	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
8	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
9	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
10	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled

CONFIGURING A REMOTE LOOP BACK TEST

Use the Administration > OAM > Remote Loopback (Remote Loopback Test) page to initiate a loop back test to the peer device attached to the selected port.

CLI REFERENCES

- ◆ ["efm oam remote-loopback" on page 1342](#)
- ◆ ["efm oam remote-loopback test" on page 1343](#)

COMMAND USAGE

- You can use this command to perform an OAM remote loop back 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 loop back mode.
- ◆ During a remote loop back 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 loop back testing.

- ◆ To perform a loopback test, first enable Remote Loop Back Mode, click Test, and then click End. The number of packets transmitted and received will be displayed.

PARAMETERS

These parameters are displayed:

Loopback Mode of Remote Device

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Loopback Mode** – Shows if loopback mode is enabled on the peer. This attribute must be enabled before starting the loopback test.
- ◆ **Loopback Status** – Shows if loopback testing is currently running.

Loopback Test Parameters

- ◆ **Packet Number** – Number of packets to send. (Range: 1-999999999; Default: 10000)
- ◆ **Packet Size** – Size of packets to send. (Range: 64-1518 bytes; Default: 64 bytes)
- ◆ **Test** – Starts the loop back test.
- ◆ **End** – Stops the loop back test.

Loop Back Status of Remote Device

- ◆ **Result** – Shows the loop back status on the peer. The loop back states shown in this field are described below.

Table 36: Remote Loopback Status

State	Description
No Loopback	Operating in normal mode with no loopback in progress.
Initiating Loopback	The local OAM entity is starting the loopback process with its peer. It has yet to receive any acknowledgement that the remote OAM entity has received its loopback command request.
Remote Loopback	The local OAM client knows that the remote OAM entity is in loopback mode.
Terminating Loopback	The local OAM client is in the process of terminating the remote loopback.
Local Loopback	The remote OAM client has put the local OAM entity in loopback mode.
Unknown	This status may be returned if the OAM loopback is in a transition state but should not persist.

- **Packets Transmitted** – The number of loop back frames transmitted during the last loopback test on this interface.

- **Packets Received** – The number of loop back frames received during the last loop back test on this interface.
- **Loss Rate** – The percentage of packets for which there was no response.

WEB INTERFACE

To initiate a loop back test to the peer device attached to the selected port:

1. Click Administration, OAM, Remote Loop Back.
2. Select Remote Loopback Test from the Action list.
3. Select the port on which to initiate remote loop back testing, enable the Loop Back Mode attribute, and click Apply.
4. Set the number of packets to send and the packet size, and then click Test.

Figure 320: Running a Remote Loop Back Test

Administration > OAM > Remote Loopback

Action: Remote Loopback Test

Port 2

Loopback Mode ☒ Enabled

Loopback Status Remote Loopback

Apply Revert

Packet Number (1-99999999)

Packet Size (64-1518) bytes

Test End

Result

10 packets transmitted. 10 packets received. Loss rate is 0.00 %

DISPLAYING RESULTS
OF REMOTE LOOP
BACK TESTING

Use the Administration > OAM > Remote Loop Back (Show Test Result) page to display the results of remote loop back testing for each port for which this information is available.

CLI REFERENCES

- ◆ "show efm oam remote-loopback interface" on page 1345

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Packets Transmitted** – The number of loop back frames transmitted during the last loop back test on this interface.

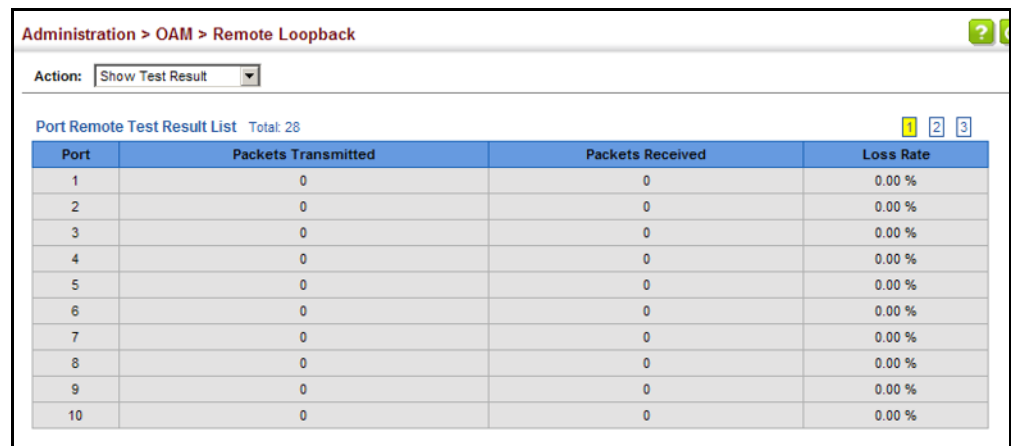
- ◆ **Packets Received** – The number of loop back frames received during the last loop back test on this interface.
- ◆ **Loss Rate** – The percentage of packets transmitted for which there was no response.

WEB INTERFACE

To display the results of remote loop back testing for each port for which this information is available:

1. Click Administration, OAM, Remote Loop Back.
2. Select Show Test Result from the Action list.

Figure 321: Displaying the Results of Remote Loop Back Testing



Administration > OAM > Remote Loopback

Action: Show Test Result

Port Remote Test Result List Total: 28

Port	Packets Transmitted	Packets Received	Loss Rate
1	0	0	0.00 %
2	0	0	0.00 %
3	0	0	0.00 %
4	0	0	0.00 %
5	0	0	0.00 %
6	0	0	0.00 %
7	0	0	0.00 %
8	0	0	0.00 %
9	0	0	0.00 %
10	0	0	0.00 %

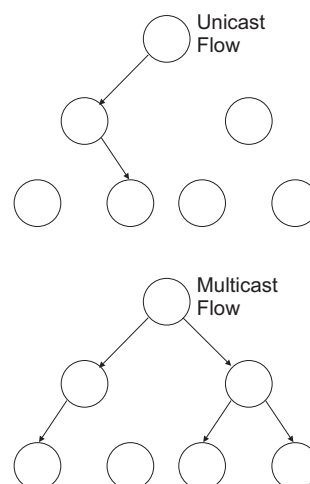
This chapter describes how to configure the following multicast services:

- ◆ **IGMP** – Configures snooping and query parameters.
- ◆ **Filtering and Throttling** – Filters specified multicast service, or throttling the maximum of multicast groups allowed on an interface.
- ◆ **Multicast VLAN Registration 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.
- ◆ **Multicast VLAN Registration 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.

OVERVIEW

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

Figure 322: Multicast Filtering Concept



This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or “snoop” on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the 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.

The purpose of IP multicast filtering is to optimize a switched network’s performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

You can also configure a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation ["Multicast VLAN Registration for IPv4" on page 584](#).

LAYER 2 IGMP (SNOOPING AND QUERY)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query ([page 560](#)) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have *not* requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source. For IGMPv1/v2 hosts, the source address of a channel is always null (indicating that any source is acceptable), but for IGMPv3 hosts, it may include a specific address when requested.

Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from any source except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.



NOTE: When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.

NOTE: IGMP snooping will not function unless a multicast router port is enabled on the switch. This can be accomplished in one of two ways. A static router port can be manually configured (see ["Specifying Static Interfaces for a Multicast Router" on page 564](#)). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

NOTE: A maximum of up to 1023 multicast entries can be maintained for IGMP snooping. Once the table is full, no new entries are learned. Any subsequent multicast traffic not found in the table is dropped if unregistered-flooding is disabled (default behavior) and no router port is configured in the attached VLAN, or flooded throughout the VLAN if unregistered-flooding is enabled (see ["Configuring IGMP Snooping and Query Parameters" on page 560](#)).

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch ([page 564](#)). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch ([page 566](#)).

IGMP Snooping with Proxy Reporting – The switch supports last leave, and query suppression (as defined in DSL Forum TR-101, April 2006):

- ◆ When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.
- ◆ Last Leave: Intercepts, absorbs and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, that is, when the last user leaves a multicast group.
- ◆ Query Suppression: Intercepts and processes IGMP queries in such a way that IGMP specific queries are never sent to client ports.

The only deviation from TR-101 is that the marking of IGMP traffic initiated by the switch with priority bits as defined in R-250 is not supported.

CONFIGURING IGMP SNOOPING AND QUERY PARAMETERS

Use the Multicast > IGMP Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

CLI REFERENCES

- ◆ ["IGMP Snooping" on page 1201](#)

COMMAND USAGE

- ◆ **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.



NOTE: If unknown multicast traffic enters a VLAN which has been configured with a router port, the traffic is forwarded to that port. However, if no router port exists on the VLAN, the traffic is dropped if unregistered data flooding is disabled (default behavior), or flooded throughout the VLAN if unregistered data flooding is enabled (see "Unregistered Data Flooding" in the Command Attributes section).

- ◆ **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.



NOTE: Multicast routers use this information from IGMP snooping and query reports, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

PARAMETERS

These parameters are displayed:

- ◆ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Enabled)

When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence (see ["Setting IGMP Snooping Status per Interface" on page 568](#)).

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.

- ◆ **Proxy Reporting Status** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)

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.

When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.

- ◆ **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

When a spanning tree topology change occurs, the multicast membership information learned by 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 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 time out 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 currently learned channels out 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 packet loss 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. Otherwise, the time spent in flooding mode can be manually configured to reduce excessive loading.

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.

- ◆ **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

When the root bridge in a spanning tree receives a TCN for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (or 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 immediately issues an IGMP general query.

A query solicitation can be sent whenever the switch notices a topology change, even if it is not the root bridge in spanning tree.

- ◆ **Router Alert Option** – Discards any IGMPv2/v3 packets that do not include the Router Alert option. (Default: Disabled)

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.

- ◆ **Unregistered Data Flooding** – Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled)

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.

- ◆ **Forwarding Priority** – Assigns a CoS priority to all multicast traffic. (Range: 0-6, where 6 is the highest priority)

This parameter 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.

- ◆ **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

- ◆ **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. (Range: 1-65535 seconds, Default: 400 seconds)

When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels via the new upstream interface.

This command only applies when proxy reporting is enabled.

- ◆ **Router Port Expire Time** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)
- ◆ **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

This attribute 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.
- ◆ **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)

WEB INTERFACE

To configure general settings for IGMP Snooping and Query:

1. Click Multicast, IGMP Snooping, General.
2. Adjust the IGMP settings as required.
3. Click Apply.

Figure 323: Configuring General Settings for IGMP Snooping

Multicast > IGMP Snooping > General	
IGMP Snooping Status	<input checked="" type="checkbox"/> Enabled
Proxy Reporting Status	<input type="checkbox"/> Enabled
TCN Flood	<input type="checkbox"/> Enabled
TCN Query Solicit	<input type="checkbox"/> Enabled
Router Alert Option	<input type="checkbox"/> Enabled
Unregistered Data Flooding	<input type="checkbox"/> Enabled
Forwarding Priority (0-6)	<input type="text" value="65535"/>
Version Exclusive	<input type="checkbox"/> Enabled
IGMP Unsolicited Report Interval (1-65535)	<input type="text" value="400"/> seconds
Router Port Expire Time (1-65535)	<input type="text" value="300"/> seconds
IGMP Snooping Version (1-3)	<input type="text" value="2"/>
Querier Status	<input type="checkbox"/> Enabled

SPECIFYING STATIC INTERFACES FOR A MULTICAST ROUTER

Use the Multicast > IGMP Snooping > Multicast Router (Add) page to statically attach an interface to a multicast router/switch.

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

CLI REFERENCES

- ◆ ["Static Multicast Routing" on page 1223](#)

COMMAND USAGE

IGMP Snooping must be enabled globally on the switch (see ["Configuring IGMP Snooping and Query Parameters" on page 560](#)) before a multicast router port can take effect.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port** or **Trunk** – Specifies the interface attached to a multicast router.
- ◆ **Type** – Shows if this entry is static or dynamic.
- ◆ **Expire** – Time until this dynamic entry expires.

WEB INTERFACE

To specify a static interface attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Add Static Multicast Router from the Action list.
3. Select the VLAN which will forward all the corresponding multicast traffic, and select the port or trunk attached to the multicast router.
4. Click Apply.

Figure 324: Configuring a Static Interface for a Multicast Router

The screenshot shows the 'Multicast > IGMP Snooping > Multicast Router' configuration page. The 'Action' dropdown is set to 'Add Static Multicast Router'. Below this, the 'VLAN' is set to '1'. The 'Interface' section has two options: 'Port' (selected with a radio button) and 'Trunk' (unselected). The 'Port' option has a dropdown menu showing '1'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the static interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Show Static Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 325: Showing Static Interfaces Attached a Multicast Router

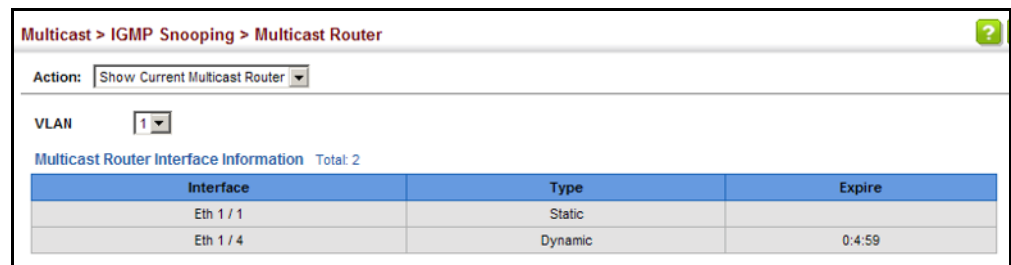
The screenshot shows the 'Multicast > IGMP Snooping > Multicast Router' configuration page. The 'Action' dropdown is set to 'Show Static Multicast Router'. Below this, the 'VLAN' is set to '1'. The page displays a table titled 'Static Multicast Router Interface List' with a 'Total: 6' count. The table has two columns: a checkbox column and an 'Interface' column. The interfaces listed are 'Unit 1 / Port 1', 'Unit 1 / Port 2', 'Unit 1 / Port 3', 'Trunk 2', 'Trunk 5', and 'Unit 1 / Port 4'. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Interface
<input type="checkbox"/>	Unit 1 / Port 1
<input type="checkbox"/>	Unit 1 / Port 2
<input type="checkbox"/>	Unit 1 / Port 3
<input type="checkbox"/>	Trunk 2
<input type="checkbox"/>	Trunk 5
<input type="checkbox"/>	Unit 1 / Port 4

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol (such as PIM) to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch. To show the all interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Current Multicast Router from the Action list.
3. Select the VLAN for which to display this information. Ports in the selected VLAN which are attached to a neighboring multicast router/ switch are displayed.

Figure 326: Showing Current Interfaces Attached a Multicast Router



Multicast Router Interface Information Total: 2		
Interface	Type	Expire
Eth 1 / 1	Static	
Eth 1 / 4	Dynamic	0:4:59

ASSIGNING INTERFACES TO MULTICAST SERVICES

Use the Multicast > IGMP Snooping > IGMP Member (Add Static Member) page to statically assign a multicast service to an interface.

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages (see ["Configuring IGMP Snooping and Query Parameters" on page 560](#)). However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

CLI REFERENCES

- ◆ ["ip igmp snooping vlan static" on page 1218](#)

COMMAND USAGE

- ◆ Static multicast addresses are never aged out.
- ◆ When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port** or **Trunk** – Specifies the interface assigned to a multicast group.
- ◆ **Multicast IP** – The IP address for a specific multicast service.

WEB INTERFACE

To statically assign an interface to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Add Static Member from the Action list.

3. Select the VLAN that will propagate the multicast service, specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), and enter the multicast IP address.
4. Click Apply.

Figure 327: Assigning an Interface to a Multicast Service

Multicast > IGMP Snooping > IGMP Member

Action: Add Static Member

VLAN: 1

Interface: ☒ Port 1 ☐ Trunk 1

Multicast IP: 224.1.1.1

Apply Revert

To show the static interfaces assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Static Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 328: Showing Static Interfaces Assigned to a Multicast Service

Multicast > IGMP Snooping > IGMP Member

Action: Show Static Member

VLAN: 1

IGMP Member Interface List Total: 6

	Interface	Multicast IP
<input type="checkbox"/>	Unit 1 / Port 1	224.1.1.1
<input type="checkbox"/>	Unit 1 / Port 2	224.1.2.2
<input type="checkbox"/>	Unit 1 / Port 3	230.1.1.1
<input type="checkbox"/>	Trunk 2	230.1.2.2
<input type="checkbox"/>	Trunk 5	239.1.1.1
<input type="checkbox"/>	Unit 1 / Port 4	239.2.2.2

Delete Revert

SETTING IGMP SNOOPING STATUS PER INTERFACE

Use the Multicast > IGMP Snooping > Interface (Configure VLAN) page to configure IGMP snooping attributes for a VLAN. To configure snooping globally, refer to ["Configuring IGMP Snooping and Query Parameters" on page 560](#).

CLI REFERENCES

- ◆ ["IGMP Snooping" on page 1201](#)

COMMAND USAGE

Multicast Router Discovery

There have been many mechanisms used in the past to identify multicast routers. This has led to interoperability issues between multicast routers and snooping switches from different vendors. In response to this problem, the Multicast Router Discovery (MRD) protocol has been developed for use by IGMP snooping and multicast routing devices. MRD is used to discover which interfaces are attached to multicast routers, allowing IGMP-enabled devices to determine where to send multicast source and group membership messages. (MRD is specified in draft-ietf-magma-mrdisc-07.)

Multicast source data and group membership reports must be received by all multicast routers on a segment. Using the group membership protocol query messages to discover multicast routers is insufficient due to query suppression. MRD therefore provides a standardized way to identify multicast routers without relying on any particular multicast routing protocol.



NOTE: The default values recommended in the MRD draft are implemented in the switch.

Multicast Router Discovery uses the following three message types to discover multicast routers:

- ◆ Multicast Router 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 occurrence of these events:
 - Upon the expiration of a periodic (randomized) timer.
 - As a part of a router's start up procedure.
 - During the restart of a multicast forwarding interface.
 - On receipt of a Solicitation message.
- ◆ Multicast Router Solicitation – 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.

- ◆ Multicast Router Termination – These messages are sent when a router stops IP multicast routing functions on an interface. Termination messages are sent by multicast routers when:
 - Multicast forwarding is disabled on an interface.
 - An interface is administratively disabled.
 - The router is gracefully shut down.

Advertisement and Termination messages are sent to the All-Snoopers multicast address. Solicitation messages are sent to the All-Routers multicast address.



NOTE: MRD messages are flooded to all ports in a VLAN where IGMP snooping or routing has been enabled. To ensure that older switches which do not support MRD can also learn the multicast router port, the switch floods IGMP general query packets, which do not have a null source address (0.0.0.0), to all ports in the attached VLAN. IGMP packets with a null source address are only flooded to all ports in the VLAN if the system is operating in multicast flooding mode, such as when a new VLAN or new router port is being established, or an spanning tree topology change has occurred. Otherwise, this kind of packet is only forwarded to known multicast routing ports.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of configured VLANs. (Range: 1-4093)
- ◆ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

When IGMP snooping is enabled globally (see [page 560](#)), 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.
- ◆ **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- ◆ **Immediate Leave Status** – 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. (Default: Disabled)

If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 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 time out period. Note that this time out is set to Last Member Query Interval * Robustness Variable (fixed at 2) as defined in RFC 2236.

If 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 IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.

- ◆ **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: Disabled)

- ◆ **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts. (Default: Disabled)

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.

- ◆ **Proxy Reporting** – Enables IGMP Snooping with Proxy Reporting. (Default: Based on global setting)

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.

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.

- ◆ **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

This attribute 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.

- ◆ **Query Interval** – The interval between sending IGMP proxy general queries. (Range: 2-31744 seconds; Default: 125 seconds)

An IGMP general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.

This attribute applies when the switch is serving as the querier ([page 560](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 560](#)).

- ◆ **Query Response Interval** – The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second; Default: 10 seconds)

This attribute applies when the switch is serving as the querier ([page 560](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 560](#)).

- ◆ **Last Member Query 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 in multiples of 10; Default: 1 second)

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 burst traffic.

This attribute will take effect only if IGMP snooping proxy reporting is enabled ([page 560](#)) or IGMP querier is enabled ([page 560](#)).

- ◆ **Last Member Query Count** – 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. (Range: 1-255; Default: 2)

This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

- ◆ **Proxy Query Address** – A static source address for locally generated query and report messages used by IGMP Proxy Reporting.
(Range: Any valid IP unicast address; Default: 0.0.0.0)

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 messages can be replaced with any valid unicast address (other than the router's own address).

WEB INTERFACE

To configure IGMP snooping on a VLAN:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure VLAN from the Action list.
3. Select the VLAN to configure and update the required parameters.
4. Click Apply.

Figure 329: Configuring IGMP Snooping on a VLAN

Multicast > IGMP Snooping > Interface

Action: Configure VLAN

VLAN: 1

IGMP Snooping Status: ☒ Enabled

Version Exclusive: ☐ Enabled

Immediate Leave Status: ☐ Enabled

Multicast Router Discovery: ☐ Enabled

General Query Suppression: ☐ Enabled

Proxy Reporting: Disabled

Interface Version (1-3): 2

Query Interval (2-31744): 125 seconds

Query Response Interval (10-31740): 100 (1/10 seconds, multiple of 10)

Last Member Query Interval (1-31744): 10 (1/10 seconds, multiple of 10)

Last Member Query Count (1-255): 2

Proxy (Query) Address: 0.0.0.0

Apply Revert

To show the interface settings for IGMP snooping:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Show VLAN Information from the Action list.

Figure 330: Showing Interface Settings for IGMP Snooping

Multicast > IGMP Snooping > Interface												
Action: Show VLAN Information												
IGMP Snooping VLAN List Total: 4												
VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Enabled	Disabled	10	100	10	2	10.1.1.1	Enabled	Enabled	Disabled	Enabled	1
2	Disabled	Disabled	10	100	10	2	20.2.2.2	Disabled	Disabled	Enabled	Disabled	3
3	Disabled	Disabled	10	100	10	2	30.3.3.3	Disabled	Enabled	Disabled	Disabled	2
10	Disabled	Disabled	10	100	10	2	100.10.10.10	Disabled	Disabled	Enabled	Disabled	1

FILTERING IGMP QUERY PACKETS AND MULTICAST DATA

Use the Multicast > IGMP Snooping > Interface (Configure Interface) page to configure an interface to drop IGMP query packets.

CLI REFERENCES

- ◆ "ip igmp query-drop" on page 1230

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or Trunk identifier.
- ◆ **IGMP Query Drop** – Configures an interface to drop any IGMP 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.

WEB INTERFACE

To drop IGMP query packets or multicast data packets:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure Interface from the Action list.
3. Select Port or Trunk interface.
4. Enable the required drop functions for any interface.
5. Click Apply.

Figure 331: Dropping IGMP Query or Multicast Data Packets

Multicast > IGMP Snooping > Interface

Action: Configure Interface

Interface ☒ Port ☐ Trunk

Port List Total: 28 1 2 3

Port	IGMP Query Drop
1	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled

DISPLAYING MULTICAST GROUPS DISCOVERED BY IGMP SNOOPING

Use the Multicast > IGMP Snooping > Forwarding Entry page to display the forwarding entries learned through IGMP Snooping.

CLI REFERENCES

- ◆ ["show ip igmp snooping group" on page 1220](#)

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see [page 560](#)).

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
- ◆ **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- ◆ **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.
- ◆ **Up Time** – Time that this multicast group has been known.
- ◆ **Expire** – Time until this entry expires.
- ◆ **Count** – The number of times this address has been learned by IGMP snooping.

WEB INTERFACE

To show multicast groups learned through IGMP snooping:

1. Click Multicast, IGMP Snooping, Forwarding Entry.
2. Select the VLAN for which to display this information.

Figure 332: Showing Multicast Groups Learned by IGMP Snooping

Multicast > IGMP Snooping > Forwarding Entry

VLAN: 1

IGMP Snooping Forwarding Entry List Total: 10

Group Address	Interface	Up Time	Expire	Count
224.1.1.1	Eth 1 / 9 (Router Port)	00:00:06:46		2 (Port)
	Eth 1 / 11 (Member Port)	00:00:06:46	03:46	1 (Host)
224.1.1.2	Eth 1 / 9 (Router Port)		02:24	1 (Port)
224.1.1.3	Eth 1 / 9 (Router Port)	00:00:16:14		1 (Port)
239.255.255.250	Eth 1 / 9 (Router Port)	00:00:08:47		2 (Port)
	Eth 1 / 11 (Member Port)	00:00:08:47	03:46	1 (Host)

Clear Click this button to clear all IGMP Snooping dynamic groups.

DISPLAYING IGMP SNOOPING STATISTICS

Use the Multicast > IGMP Snooping > Statistics pages to display IGMP snooping protocol-related statistics for the specified interface.

CLI REFERENCES

- ◆ ["show ip igmp snooping statistics" on page 1221](#)

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk identifier. (Range: 1-16)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **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.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **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, packet content not allowed, or IGMP group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of IGMP groups active on this interface.

Output Statistics

- ◆ **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.

WEB INTERFACE

To display statistics for IGMP snooping query-related messages:

1. Click Multicast, IGMP Snooping, Statistics.
2. Select Show Query Statistics from the Action list.
3. Select a VLAN.

Figure 333: Displaying IGMP Snooping Statistics – Query

The screenshot shows the 'Multicast > IGMP Snooping > Statistics' web interface. At the top, there is a breadcrumb trail. Below it, an 'Action:' dropdown menu is set to 'Show Query Statistics'. A 'VLAN' dropdown menu is set to '1'. The main content area is titled 'Query Statistics' and displays a table of statistics for the selected VLAN. The table includes the following data:

Querier IP Address	192.168.1.1
Querier Expire Time	00:00:00
General Query Received	0
General Query Sent	8
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	2
Number of Leaves Sent	2

At the bottom of the interface, there is a 'Clear All' button with a tooltip that says 'Click this button to clear all IGMP Snooping statistics.' and a 'Refresh' button.

To display IGMP snooping protocol-related statistics for a VLAN:

1. Click Multicast, IGMP Snooping, Statistics.
2. Select Show VLAN Statistics from the Action list.
3. Select a VLAN.

Figure 334: Displaying IGMP Snooping Statistics – VLAN

The screenshot shows the 'Multicast > IGMP Snooping > Statistics' page. The 'Action' dropdown is set to 'Show VLAN Statistics'. The 'VLAN' dropdown is set to '1'. The page displays two sections: 'Input Statistics' and 'Output Statistics'. The 'Input Statistics' section shows values for Report (0), Leave (0), G Query (0), G(-S)-S Query (0), Drop (0), Join Success (0), and Group (0). The 'Output Statistics' section shows values for Report (18), Leave (0), G Query (0), and G(-S)-S Query (0). A 'Refresh' button is located at the bottom right.

Multicast > IGMP Snooping > Statistics			
Action: Show VLAN Statistics			
VLAN: 1			
Input Statistics			
Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		
Output Statistics			
Report	18		
Leave	0		
G Query	0		
G(-S)-S Query	0		
Refresh			

To display IGMP snooping protocol-related statistics for a port:

1. Click Multicast, IGMP Snooping, Statistics.
2. Select Show Port Statistics from the Action list.
3. Select a Port.

Figure 335: Displaying IGMP Snooping Statistics – Port

The screenshot shows the 'Multicast > IGMP Snooping > Statistics' page. The 'Action' dropdown is set to 'Show Port Statistics'. The 'Port' dropdown is set to '1'. The page displays two sections: 'Input Statistics' and 'Output Statistics'. The 'Input Statistics' section shows values for Report (0), Leave (0), G Query (0), G(-S)-S Query (0), Drop (0), Join Success (0), and Group (0). The 'Output Statistics' section shows values for Report (0), Leave (0), G Query (0), and G(-S)-S Query (0). A 'Refresh' button is located at the bottom right.

Multicast > IGMP Snooping > Statistics			
Action: Show Port Statistics			
Port: 1			
Input Statistics			
Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		
Output Statistics			
Report	0		
Leave	0		
G Query	0		
G(-S)-S Query	0		
Refresh			

FILTERING AND THROTTLING IGMP GROUPS

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.

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 addresses, 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 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 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.

ENABLING IGMP FILTERING AND THROTTLING

Use the Multicast > IGMP Snooping > Filter (Configure General) page to enable IGMP filtering and throttling globally on the switch.

CLI REFERENCES

- ◆ ["ip igmp filter \(Global Configuration\)" on page 1225](#)

PARAMETERS

These parameters are displayed:

- ◆ **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

WEB INTERFACE

To enable IGMP filtering and throttling on the switch:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure General from the Step list.
3. Enable IGMP Filter Status.
4. Click Apply.

Figure 336: Enabling IGMP Filtering and Throttling

Multicast > IGMP Snooping > Filter

Step: 1. Configure General

IGMP Filter Status ☒ Enabled

Apply Revert

CONFIGURING IGMP FILTER PROFILES

Use the Multicast > IGMP Snooping > Filter (Configure Profile – Add) page to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.

CLI REFERENCES

- ◆ ["IGMP Filtering and Throttling" on page 1225](#)

COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

PARAMETERS

These parameters are displayed:

Add

- ◆ **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)
- ◆ **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: 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 the multicast group is not in the controlled range.

Add Multicast Group Range

- ◆ **Profile ID** – Selects an IGMP profile to configure.
- ◆ **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- ◆ **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

WEB INTERFACE

To create an IGMP filter profile and set its access mode:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Add from the Action list.
4. Enter the number for a profile, and set its access mode.
5. Click Apply.

Figure 337: Creating an IGMP Filtering Profile

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add

Profile ID (1-4294967295) 19

Access Mode Permit

Apply Revert

To show the IGMP filter profiles:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Show from the Action list.

Figure 338: Showing the IGMP Filtering Profiles Created

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show

IGMP Snooping Filter Profile List Total: 1

	Profile ID	Action Mode
<input type="checkbox"/>	19	Permit

Delete Revert

To add a range of multicast groups to an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Add Multicast Group Range from the Action list.
4. Select the profile to configure, and add a multicast group address or range of addresses.

5. Click Apply.

Figure 339: Adding Multicast Groups to an IGMP Filtering Profile

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add Multicast Group Range

Profile ID: 19

Start Multicast IP Address: 239.2.3.1

End Multicast IP Address: 239.2.3.200

Apply Revert

To show the multicast groups configured for an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Show Multicast Group Range from the Action list.
4. Select the profile for which to display this information.

Figure 340: Showing the Groups Assigned to an IGMP Filtering Profile

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show Multicast Group Range

Profile ID: 19

Multicast IP Address Range List Total: 1

	Start Multicast IP Address	End Multicast IP Address
<input type="checkbox"/>	239.2.3.1	239.2.3.200

Delete Revert

CONFIGURING IGMP FILTERING AND THROTTLING FOR INTERFACES

Use the Multicast > IGMP Snooping > Filter (Configure Interface) page to assign an IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

CLI REFERENCES

- ◆ ["IGMP Filtering and Throttling" on page 1225](#)

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." 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.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or trunk identifier.
An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.
- ◆ **Profile ID** – Selects an existing profile to assign to an interface.
- ◆ **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 1-1023; Default: 1023)
- ◆ **Current Multicast Groups** – Displays the current multicast groups the interface has joined.
- ◆ **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)
 - **Deny** - The new multicast group join report is dropped.
 - **Replace** - The new multicast group replaces an existing group.
- ◆ **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

WEB INTERFACE

To configure IGMP filtering or throttling for a port or trunk:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Interface from the Step list.
3. Select a profile to assign to an interface, then set the maximum number of allowed multicast groups and the throttling response.
4. Click Apply.

Figure 341: Configuring IGMP Filtering and Throttling Interface Settings

Multicast > IGMP Snooping > Filter

Step: 3. Configure Interface

Interface ☒ Port ☐ Trunk

IGMP Filter and Throttling Port List Total: 28

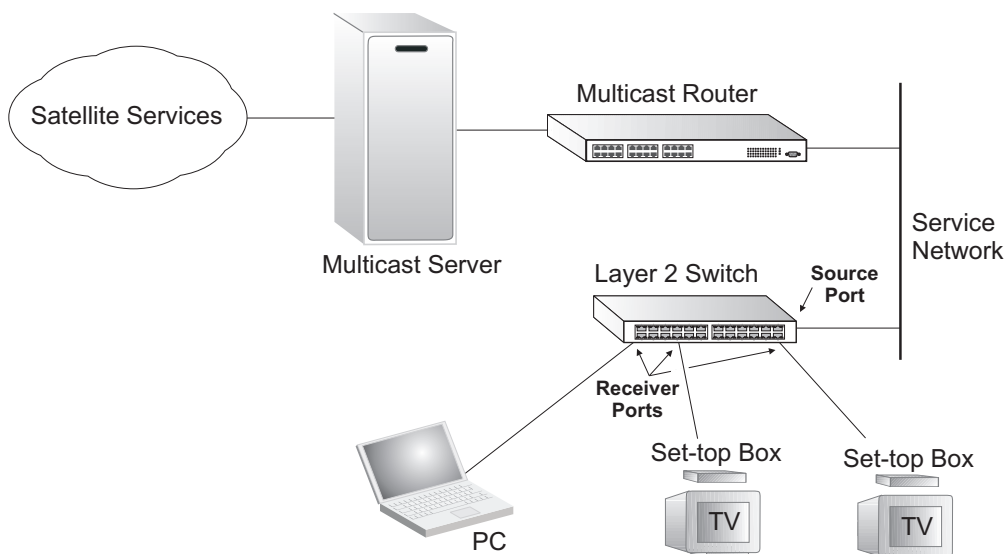
Port	Profile ID	Max Multicast Groups (1-1023)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	19	64	0	Deny	False
2	(none)	1023	0	Deny	False
3	(none)	1023	0	Deny	False
4	(none)	1023	0	Deny	False
5	(none)	1023	0	Deny	False

MULTICAST VLAN REGISTRATION FOR IPv4

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast routing protocol.

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. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

Figure 342: MVR Concept



COMMAND USAGE

◆ General Configuration Guidelines for MVR:

1. Enable MVR for a domain on the switch, and select the MVR VLAN (see ["Configuring MVR Domain Settings" on page 587](#)).
2. Create an MVR profile by specifying the multicast groups that will stream traffic to attached hosts, and assign the profile to an MVR domain (see ["Configuring MVR Group Address Profiles" on page 589](#)).
3. Set the interfaces that will join the MVR as source ports or receiver ports (see ["Configuring MVR Interface Status" on page 592](#)).
4. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see ["Assigning Static MVR Multicast Groups to Interfaces" on page 594](#)).

- ◆ Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping. Also, note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

CONFIGURING MVR GLOBAL SETTINGS Use the Multicast > MVR (Configure Global) page to configure proxy switching and the robustness variable.

CLI REFERENCES

- ◆ ["MVR for IPv4" on page 1233](#)

PARAMETERS

These parameters are displayed:

- ◆ **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
 - When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. 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.
- ◆ **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-255; Default: 2)
 - This parameter 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 parameter only takes effect when MVR proxy switching is enabled.
- ◆ **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
 - This parameter sets the general query interval at which active receiver ports send out general queries.
 - This interval is only effective when proxy switching is enabled.
- ◆ **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.
 - **Always Forward** – 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. (This is the default setting.)
 - **Dynamic** – When dynamic mode is enabled, 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.

WEB INTERFACE

To configure global settings for MVR:

1. Click Multicast, MVR.
2. Select Configure Global from the Step list.
3. Set the status for MVR proxy switching, the robustness value used for report and query messages, the proxy query interval, and source port mode.
4. Click Apply.

Figure 343: Configuring Global Settings for MVR

The screenshot shows the 'Multicast > MVR' configuration page. At the top, there is a 'Step:' dropdown menu set to '1. Configure Global'. Below this, there are four configuration items: 'Proxy Switching' with a checked checkbox and the text 'Enabled'; 'Robustness Value (1-255)' with a text input field containing '1'; 'Proxy Query Interval (2-31744)' with a text input field containing '125' and a 'sec' label; and 'Source Port Mode' with a dropdown menu set to 'Always Forward'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

CONFIGURING MVR DOMAIN SETTINGS

Use the Multicast > MVR (Configure Domain) page to enable MVR globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

CLI REFERENCES

- ◆ ["MVR for IPv4" on page 1233](#)

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- ◆ **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see ["Adding Static Members to VLANs" on page 199](#)), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)

- ◆ **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a source port with a valid link has been configured (see ["Configuring MVR Interface Status" on page 592](#)).
- ◆ **MVR Current Learned Groups** – The number of MVR groups currently assigned to this domain.
- ◆ **Forwarding Priority** – The CoS priority assigned to all multicast traffic forwarded into this domain. (Range: 0-6, where 6 is the highest priority)

This parameter 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.
- ◆ **Upstream Source IP** – The source IP address assigned to all MVR control packets sent upstream on the specified domain. By default, all MVR reports sent upstream use a null source IP address.

WEB INTERFACE

To configure settings for an MVR domain:

1. Click Multicast, MVR.
2. Select Configure Domain from the Step list.
3. Select a domain from the scroll-down list.
4. Enable MVR for the selected domain, select the MVR VLAN, set the forwarding priority to be assigned to all ingress multicast traffic, and set the source IP address for all control packets sent upstream as required.
5. Click Apply.

Figure 344: Configuring Domain Settings for MVR

The screenshot shows a web interface for configuring MVR settings. The breadcrumb is "Multicast > MVR". The "Step:" dropdown is set to "2. Configure Domain". The configuration fields are as follows:

Field	Value
Domain ID	1
MVR Status	<input checked="" type="checkbox"/> Enabled
MVR VLAN	1
MVR Running Status	Active
MVR Current Learned Groups	0
Forwarding Priority (0-6)	<input type="checkbox"/> <input type="text"/>
Upstream Source IP	192.168.0.12

At the bottom right, there are "Apply" and "Revert" buttons.

CONFIGURING MVR GROUP ADDRESS PROFILES

Use the Multicast > MVR (Configure Profile and Associate Profile) pages to assign the multicast group address for required services to one or more MVR domains.

CLI REFERENCES

- ◆ ["MVR for IPv4" on page 1233](#)

COMMAND USAGE

- ◆ Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with 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.

PARAMETERS

These parameters are displayed:

Configure Profile

- ◆ **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- ◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- ◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-21 characters)

WEB INTERFACE

To configure an MVR group address profile:

1. Click Multicast, MVR.
2. Select Configure Profile from the Step list.
3. Select Add from the Action list.
4. Enter the name of a group profile to be assigned to one or more domains, and specify a multicast group that will stream traffic to participating hosts.
5. Click Apply.

Figure 345: Configuring an MVR Group Address Profile

The screenshot shows the 'Multicast > MVR' configuration page. At the top, there's a breadcrumb 'Multicast > MVR'. Below it, a 'Step:' dropdown is set to '2. Configure Profile' and an 'Action:' dropdown is set to 'Add'. The main form has three input fields: 'Profile Name' with the value 'sales', 'Start IP Address' with the value '234.5.6.8', and 'End IP Address' with the value '234.5.6.10'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the configured MVR group address profiles:

1. Click Multicast, MVR.
2. Select Configure Profile from the Step list.
3. Select Show from the Action list.

Figure 346: Displaying MVR Group Address Profiles

The screenshot shows the 'Multicast > MVR' configuration page. At the top, there's a breadcrumb 'Multicast > MVR'. Below it, a 'Step:' dropdown is set to '2. Configure Profile' and an 'Action:' dropdown is set to 'Show'. Below the dropdowns, there's a section titled 'MVR Profile List' with a 'Total: 2' indicator. It contains a table with the following data:

	Profile Name	Start IP Address	End IP Address
<input type="checkbox"/>	sales	234.5.6.8	234.5.6.10
<input type="checkbox"/>	rd	234.5.6.7	234.5.6.7

At the bottom right, there are 'Delete' and 'Revert' buttons.

To assign an MVR group address profile to a domain:

1. Click Multicast, MVR.
2. Select Associate Profile from the Step list.
3. Select Add from the Action list.
4. Select a domain from the scroll-down list, and enter the name of a group profile.
5. Click Apply.

Figure 347: Assigning an MVR Group Address Profile to a Domain

Multicast > MVR

Step: 4. Associate Profile Action: Add

Domain ID: 1

Profile Name: sales

Apply Revert

To show the MVR group address profiles assigned to a domain:

1. Click Multicast, MVR.
2. Select Associate Profile from the Step list.
3. Select Show from the Action list.

Figure 348: Showing the MVR Group Address Profiles Assigned to a Domain

Multicast > MVR

Step: 3. Associate Profile Action: Show

Domain ID: 1

Domain Associated Profile List Total: 2

<input type="checkbox"/>	Profile Name	Start IP Address	End IP Address
<input type="checkbox"/>	rd	234.5.6.7	234.5.6.7
<input type="checkbox"/>	sales	234.5.6.8	234.5.6.10

Delete Revert

CONFIGURING MVR INTERFACE STATUS

Use the Multicast > MVR (Configure Interface) page to configure each interface that participates in the MVR protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

CLI REFERENCES

- ◆ ["MVR for IPv4" on page 1233](#)

COMMAND USAGE

- ◆ A port configured as an MVR receiver or source port can join or leave multicast groups configured under MVR. However, note that these ports can also use IGMP snooping to join or leave any other multicast groups using the standard rules for multicast filtering.

- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. MVR allows a receiver port to dynamically join or leave multicast groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port (see ["Assigning Static MVR Multicast Groups to Interfaces" on page 594](#)).

Receiver ports should not be statically configured as a member of the MVR VLAN. If so configured, its MVR status will be inactive. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see ["Adding Static Members to VLANs" on page 199](#)).

- ◆ One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for configured MVR groups or for groups which have been statically assigned (see ["Assigning Static MVR Multicast Groups to Interfaces" on page 594](#)).

All source ports must belong to the MVR VLAN.

Subscribers should not be directly connected to source ports.

- ◆ 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 query message 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.
 - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to 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.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Port/Trunk** – Interface identifier.

- ◆ **Type** – The following interface types are supported:
 - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN (see ["Adding Static Members to VLANs" on page 199](#)).
 - **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that 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 (see ["Assigning Static MVR Multicast Groups to Interfaces" on page 594](#)).
 - **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)
- ◆ **Forwarding Status** – Shows if MVR traffic is being forwarded or discarded.
- ◆ **MVR Status** – Shows the MVR 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.
- ◆ **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)

WEB INTERFACE

To configure interface settings for MVR:

1. Click Multicast, MVR.
2. Select Configure Interface from the Step list.
3. Select Configure Port or Configure Trunk from the Action list.
4. Select an MVR domain.
5. Set each port that will participate in the MVR protocol as a source port or receiver port, and optionally enable Immediate Leave on any receiver port to which only one subscriber is attached.
6. Click Apply.

Figure 349: Configuring Interface Settings for MVR

Multicast > MVR

Step: 4. Configure Interface Action: Configure Port

Domain ID: 1

Port List Total: 28

Port	Type	Forwarding Status	MVR Status	Immediate Leave
1	Source	Forwarding	Inactive	<input type="checkbox"/> Enabled
2	Receiver	Discarding	Inactive	<input checked="" type="checkbox"/> Enabled
3	Non-MVR	Discarding	Inactive	<input type="checkbox"/> Enabled
4	Non-MVR	Discarding	Inactive	<input type="checkbox"/> Enabled
5	Non-MVR	Discarding	Inactive	<input type="checkbox"/> Enabled

ASSIGNING STATIC MVR MULTICAST GROUPS TO INTERFACES

Use the Multicast > MVR (Configure Static Group Member) page to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

CLI REFERENCES

- ◆ ["mvr vlan group" on page 1243](#)

COMMAND USAGE

- ◆ Multicast groups can be statically assigned to a receiver port using this configuration page.
- ◆ 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.
- ◆ The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

WEB INTERFACE

To assign a static MVR group to an interface:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Add from the Action list.
4. Select an MVR domain.
5. Select a VLAN and interface to receive the multicast stream, and then enter the multicast group address.
6. Click Apply.

Figure 350: Assigning Static MVR Groups to a Port

The screenshot shows a web interface for configuring Multicast VLAN Registration (MVR). The breadcrumb trail is "Multicast > MVR". The "Step" dropdown is set to "5. Configure Static Group Member" and the "Action" dropdown is set to "Add". The configuration fields are as follows:

Field	Value
Domain ID	1
Interface	Port 2
VLAN	2
Group IP Address	234.5.6.8

At the bottom right, there are two buttons: "Apply" and "Revert".

To show the static MVR groups assigned to an interface:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Show from the Action list.
4. Select an MVR domain.
5. Select the port or trunk for which to display this information.

Figure 351: Showing the Static MVR Groups Assigned to a Port

The screenshot shows the 'Multicast > MVR' configuration page. At the top, there's a breadcrumb 'Multicast > MVR'. Below it, a 'Step' dropdown is set to '5. Configure Static Group Member' and an 'Action' dropdown is set to 'Show'. The 'Domain ID' is set to '1'. The 'Interface' section has 'Port' selected with '2' in the dropdown, and 'Trunk' is also visible. Below this, the 'MVR Static Group Member List' is shown with a 'Total 3' count. The list is a table with three columns: a checkbox, 'VLAN', and 'Group IP Address'. There are three entries, all with 'VLAN' 2 and 'Group IP Address' values 234.5.6.8, 234.5.6.9, and 234.5.6.10. At the bottom right of the table are 'Delete' and 'Revert' buttons.

	VLAN	Group IP Address
<input type="checkbox"/>	2	234.5.6.8
<input type="checkbox"/>	2	234.5.6.9
<input type="checkbox"/>	2	234.5.6.10

DISPLAYING MVR RECEIVER GROUPS

Use the Multicast > MVR (Show Member) page to show the multicast groups either statically or dynamically assigned to the MVR receiver groups on each interface.

CLI REFERENCES

- ◆ ["show mvr" on page 1244](#)

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Group IP Address** – Multicast groups assigned to the MVR VLAN.
- ◆ **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned.
- ◆ **Port** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.
- ◆ **Up Time** – Time this service has been forwarded to attached clients.
- ◆ **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- ◆ **Count** – The number of multicast services currently being forwarded from the MVR VLAN.

WEB INTERFACE

To display the interfaces assigned to the MVR receiver groups:

1. Click Multicast, MVR.
2. Select Show Member from the Step list.
3. Select an MVR domain.

Figure 352: Displaying MVR Receiver Groups

Multicast > MVR

Step: 6. Show Member

Domain ID: 1

MVR Member List Total: 8

Group IP Address	VLAN	Port	Up Time	Expire	Count
224.1.1.1	2		00:00:30		2 (Port)
	2	Unit 1 / Port 1 (Source)			
224.1.1.2	1	Unit 1 / Port 2 (Receiver)	00:01:10	00:00	4 (Host)
	4		00:00:50		4 (Port)
	4	Unit 1 / Port 3 (Source)			
	5	Unit 1 / Port 4 (Receiver)			
	6	Unit 1 / Port 5 (Source)			
	7	Unit 1 / Port 6 (Receiver)	00:01:10	00:00	1 (Host)

DISPLAYING MVR STATISTICS Use the Multicast > MVR > Show Statistics pages to display MVR protocol-related statistics for the specified interface.

CLI REFERENCES

- ◆ ["show mvr statistics" on page 1249](#)

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk identifier. (Range: 1-16)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **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.

- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **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, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

Output Statistics

- ◆ **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.

WEB INTERFACE

To display statistics for MVR query-related messages:

1. Click Multicast, MVR.
2. Select Show Statistics from the Step list.
3. Select Show Query Statistics from the Action list.
4. Select an MVR domain.

Figure 353: Displaying MVR Statistics – Query

Multicast > MVR

Step: 7. Show Statistics Action: Show Query Statistics

Domain ID 1

Query Statistics

Querier IP Address	None
Querier Expire Time	00(h):00(m):00(s)
General Query Received	0
General Query Sent	0
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	0
Number of Leaves Sent	0

Clear All [Click this button to clear all MVR statistics of the domain.](#)

Refresh

To display MVR protocol-related statistics for a VLAN:

1. Click Multicast, MVR.
2. Select Show Statistics from the Step list.
3. Select Show VLAN Statistics from the Action list.
4. Select an MVR domain.
5. Select a VLAN.

Figure 354: Displaying MVR Statistics – VLAN

The screenshot shows the 'Multicast > MVR' configuration page. At the top, there are two dropdown menus: 'Step:' set to '7. Show Statistics' and 'Action:' set to 'Show VLAN Statistics'. Below these are two more dropdown menus: 'Domain ID' set to '1' and 'VLAN' set to '1'. The main content area is divided into two sections: 'Input Statistics' and 'Output Statistics'. Each section contains a table of statistics.

Input Statistics			
Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics	
Report	0
Leave	0
G Query	0
G(-S)-S Query	0

At the bottom right of the statistics area is a 'Refresh' button.

To display MVR protocol-related statistics for a port:

1. Click Multicast, MVR.
2. Select Show Statistics from the Step list.
3. Select Show Port Statistics from the Action list.
4. Select an MVR domain.
5. Select a Port.

Figure 355: Displaying MVR Statistics – Port

Multicast > MVR

Step: 7. Show Statistics Action: Show Port Statistics

Domain ID1

Port1

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Leave	0
G Query	0
G(-S)-S Query	0

Refresh

MULTICAST VLAN REGISTRATION FOR IPV6

MVR6 functions in a manner similar to that described for MRV (see ["Multicast VLAN Registration for IPv4" on page 584](#)).

COMMAND USAGE

◆ General Configuration Guidelines for MVR6:

1. Enable MVR6 for a domain on the switch, and select the MVR VLAN (see ["Configuring MVR6 Domain Settings" on page 604](#)).
2. Create an MVR6 profile by specifying the multicast groups that will stream traffic to attached hosts, and assign the profile to an MVR6 domain (see ["Configuring MVR6 Group Address Profiles" on page 605](#)).
3. Set the interfaces that will join the MVR as source ports or receiver ports (see ["Configuring MVR6 Interface Status" on page 608](#)).
4. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see ["Assigning Static MVR6 Multicast Groups to Interfaces" on page 610](#)).

CONFIGURING MVR6 GLOBAL SETTINGS Use the Multicast > MVR6 (Configure Global) page to configure proxy switching and the robustness variable.

CLI REFERENCES

- ◆ ["MVR for IPv6" on page 1252](#)

PARAMETERS

These parameters are displayed:

- ◆ **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
 - When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. 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.
- ◆ **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-10; Default: 2)
 - This parameter 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 parameter only takes effect when MVR6 proxy switching is enabled.

- ◆ **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
 - This parameter sets the general query interval at which active receiver ports send out general queries.
 - This interval is only effective when proxy switching is enabled.
- ◆ **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.
 - **Always Forward** – 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.
 - **Dynamic** – When dynamic mode is enabled, 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.

WEB INTERFACE

To configure global settings for MVR6:

1. Click Multicast, MVR6.
2. Select Configure Global from the Step list.
3. Set the status for MVR6 proxy switching, the robustness value used for report and query messages, the proxy query interval, and source port mode.
4. Click Apply.

Figure 356: Configuring Global Settings for MVR6

The screenshot shows a web interface for configuring MVR6 settings. The breadcrumb is 'Multicast > MVR6'. Below it, a 'Step:' dropdown menu is set to '1. Configure Global'. The configuration area contains four settings: 'Proxy Switching' is checked and set to 'Enabled'; 'Robustness Value (1-10)' is a text input with the value '1'; 'Proxy Query Interval (2-31744)' is a text input with the value '125' followed by 'sec'; and 'Source Port Mode' is a dropdown menu set to 'Always Forward'. At the bottom right, there are 'Apply' and 'Revert' buttons.

CONFIGURING MVR6 DOMAIN SETTINGS

Use the Multicast > MVR6 (Configure Domain) page to enable MVR6 globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

CLI REFERENCES

- ◆ ["MVR for IPv6" on page 1252](#)

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID**– An independent multicast domain. (Range: 1-5)
- ◆ **MVR6 Status** – When MVR6 is enabled on the switch, 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. (Default: Disabled)
- ◆ **MVR6 VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR6. MVR6 source ports should be configured as members of the MVR6 VLAN (see ["Adding Static Members to VLANs" on page 199](#)), but MVR6 receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- ◆ **MVR6 Running Status** – Indicates whether or not all necessary conditions in the MVR6 environment are satisfied. Running status is Active as long as MVR6 is enabled, the specified MVR6 VLAN exists, and a source port with a valid link has been configured (see ["Configuring MVR6 Interface Status" on page 608](#)).
- ◆ **MVR6 Current Learned Groups** – The number of MVR6 groups currently assigned to this domain.
- ◆ **Upstream Source IPv6** – The source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. This parameter must be a full IPv6 address including the network prefix and host address bits. By default, all MVR6 reports sent upstream use a null source IP address.

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.)

WEB INTERFACE

To configure settings for an MVR6 domain:

1. Click Multicast, MVR6.
2. Select Configure Domain from the Step list.
3. Select a domain from the scroll-down list.

4. Enable MVR6 for the selected domain, select the MVR6 VLAN, set the forwarding priority to be assigned to all ingress multicast traffic, and set the source IP address for all control packets sent upstream as required.
5. Click Apply.

Figure 357: Configuring Domain Settings for MVR6

The screenshot shows the 'Multicast > MVR6' configuration page. At the top, there's a 'Step:' dropdown menu set to '1. Configure Domain'. Below this, several configuration fields are listed: 'Domain ID' is a dropdown menu set to '1'; 'MVR6 Status' is a checkbox labeled 'Enabled' which is checked; 'MVR6 VLAN' is a dropdown menu set to '1'; 'MVR6 Running Status' is a text field showing 'Active'; 'MVR6 Current Learned Groups' is a text field showing '0'; and 'Upstream Source IPv6' is a text field containing the address '2001:DB8:2222:7223::72'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

CONFIGURING MVR6 GROUP ADDRESS PROFILES

Use the Multicast > MVR6 (Configure Profile and Associate Profile) pages to assign the multicast group address for required services to one or more MVR6 domains.

CLI REFERENCES

- ◆ ["MVR for IPv6" on page 1252](#)

COMMAND USAGE

- ◆ Use the Configure Profile page 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 to all receiver ports that have registered to receive data from that multicast group.
- ◆ 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.
- ◆ 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.

PARAMETERS

These parameters are displayed:

Configure Profile

- ◆ **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)
- ◆ **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- ◆ **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

WEB INTERFACE

To configure an MVR6 group address profile:

1. Click Multicast, MVR6.
2. Select Configure Profile from the Step list.
3. Select Add from the Action list.
4. Enter the name of a group profile to be assigned to one or more domains, and specify a multicast group that will stream traffic to participating hosts.
5. Click Apply.

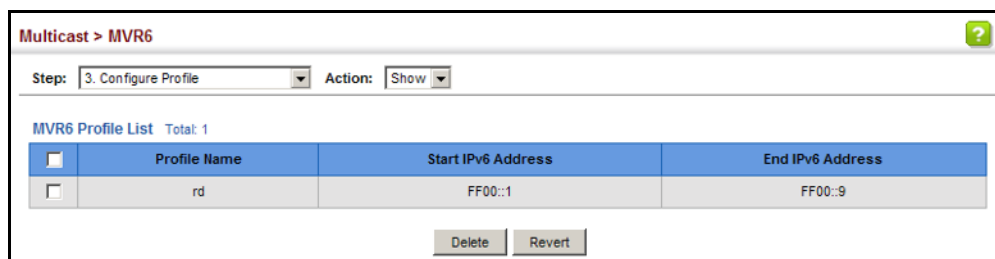
Figure 358: Configuring an MVR6 Group Address Profile

The screenshot shows a web interface for configuring an MVR6 group address profile. The breadcrumb is "Multicast > MVR6". The "Step:" dropdown is set to "2. Configure Profile" and the "Action:" dropdown is set to "Add". There are three input fields: "Profile Name" with the value "rd", "Start IPv6 Address" with the value "ff00::1", and "End IPv6 Address" with the value "ff00::9". At the bottom right, there are two buttons: "Apply" and "Revert".

To show the configured MVR6 group address profiles:

1. Click Multicast, MVR6.
2. Select Configure Profile from the Step list.
3. Select Show from the Action list.

Figure 359: Displaying MVR6 Group Address Profiles



The screenshot shows the 'Multicast > MVR6' configuration page. At the top, there is a breadcrumb 'Multicast > MVR6'. Below it, there are two dropdown menus: 'Step: 3. Configure Profile' and 'Action: Show'. The main content area is titled 'MVR6 Profile List Total: 1'. It contains a table with the following data:

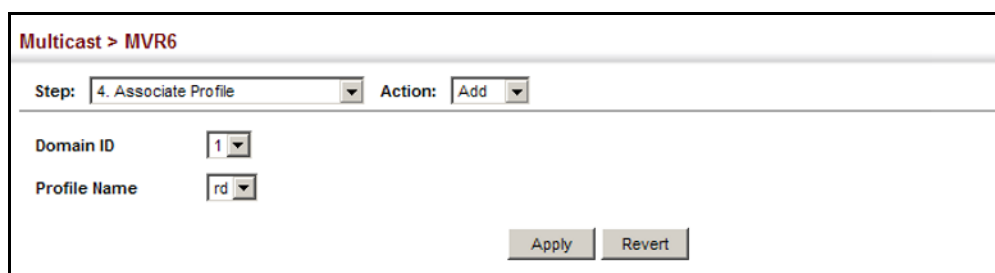
<input type="checkbox"/>	Profile Name	Start IPv6 Address	End IPv6 Address
<input type="checkbox"/>	rd	FF00::1	FF00::9

At the bottom of the table, there are two buttons: 'Delete' and 'Revert'.

To assign an MVR6 group address profile to a domain:

1. Click Multicast, MVR6.
2. Select Associate Profile from the Step list.
3. Select Add from the Action list.
4. Select a domain from the scroll-down list, and enter the name of a group profile.
5. Click Apply.

Figure 360: Assigning an MVR6 Group Address Profile to a Domain



The screenshot shows the 'Multicast > MVR6' configuration page. At the top, there is a breadcrumb 'Multicast > MVR6'. Below it, there are two dropdown menus: 'Step: 4. Associate Profile' and 'Action: Add'. The main content area has two dropdown menus: 'Domain ID' with the value '1' and 'Profile Name' with the value 'rd'. At the bottom, there are two buttons: 'Apply' and 'Revert'.

To show the MVR6 group address profiles assigned to a domain:

1. Click Multicast, MVR6.
2. Select Associate Profile from the Step list.
3. Select Show from the Action list.

Figure 361: Showing MVR6 Group Address Profiles Assigned to a Domain

Multicast > MVR6

Step: 3. Associate Profile Action: Show

Domain ID: 1

Domain Associated Profile List Total: 1

<input type="checkbox"/>	Profile Name	Start IPv6 Address	End IPv6 Address
<input type="checkbox"/>	rd	FF00::1	FF00::9

Buttons: Delete, Revert

CONFIGURING MVR6 INTERFACE STATUS

Use the Multicast > MVR6 (Configure Interface) page to configure each interface that participates in the MVR6 protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

CLI REFERENCES

- ◆ ["MVR for IPv6" on page 1252](#)

COMMAND USAGE

- ◆ A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6.
- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR6 VLAN. MVR6 allows a receiver port to dynamically join or leave multicast groups within an MVR6 VLAN. Multicast groups can also be statically assigned to a receiver port (see ["Assigning Static MVR Multicast Groups to Interfaces" on page 594](#)).

Receiver ports should not be statically configured as a member of the MVR6 VLAN. If so configured, its MVR6 status will be inactive. Also, note that VLAN membership for MVR6 receiver ports cannot be set to access mode (see ["Adding Static Members to VLANs" on page 199](#)).

- ◆ One or more interfaces may be configured as MVR6 source ports. A source port is able to both receive and send data for configured MVR6 groups or for groups which have been statically assigned (see ["Assigning Static MVR Multicast Groups to Interfaces" on page 594](#)).

All source ports must belong to the MVR6 VLAN.

Subscribers should not be directly connected to source ports.

- ◆ 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.
 - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to 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.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Port/Trunk** – Interface identifier.
- ◆ **Type** – The following interface types are supported:
 - **Non-MVR6** – An interface that does not participate in the MVR6 VLAN. (This is the default type.)
 - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR6 VLAN. Note that the source port must be manually configured as a member of the MVR6 VLAN (see ["Adding Static Members to VLANs" on page 199](#)).
 - **Receiver** – A subscriber port that can receive multicast data sent through the MVR6 VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see ["Adding Static Members to VLANs" on page 199](#)).
- ◆ **Forwarding Status** – Shows if multicast traffic is being forwarded or blocked.
- ◆ **MVR6 Status** – Shows the MVR6 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.
- ◆ **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR6 receiver.)

WEB INTERFACE

To configure interface settings for MVR6:

1. Click Multicast, MVR6.
2. Select Configure Interface from the Step list.
3. Select Configure Port or Configure Trunk from the Action list.
4. Select an MVR6 domain.

5. Set each port that will participate in the MVR6 protocol as a source port or receiver port, and optionally enable Immediate Leave on any receiver port to which only one subscriber is attached.
6. Click Apply.

Figure 362: Configuring Interface Settings for MVR6

Multicast > MVR6

Step: 4. Configure Interface Action: Configure Port

Domain ID: 1

Port List Total: 28

Port	Type	Forwarding Status	MVR6 Status	Immediate Leave
1	Source	Forwarding	Inactive	<input type="checkbox"/> Enabled
2	Receiver	Discarding	Inactive	<input type="checkbox"/> Enabled
3	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> Enabled
4	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> Enabled
5	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> Enabled

ASSIGNING STATIC MVR6 MULTICAST GROUPS TO INTERFACES

Use the Multicast > MVR6 (Configure Static Group Member) page to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

CLI REFERENCES

- ◆ ["mvr6 vlan group" on page 1261](#)

COMMAND USAGE

- ◆ Multicast groups can be statically assigned to a receiver port using this configuration page.
- ◆ 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.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

WEB INTERFACE

To assign a static MVR6 group to an interface:

1. Click Multicast, MVR6.
2. Select Configure Static Group Member from the Step list.
3. Select Add from the Action list.
4. Select an MVR6 domain.
5. Select a VLAN and interface to receive the multicast stream, and then enter the multicast group address.
6. Click Apply.

Figure 363: Assigning Static MVR6 Groups to a Port

The screenshot shows the 'Multicast > MVR6' configuration page. The 'Step' dropdown is set to '5. Configure Static Group Member' and the 'Action' dropdown is set to 'Add'. The configuration fields are as follows:

- Domain ID: 1
- Interface: Port 2 (selected), Trunk (unselected)
- VLAN: 2
- Group IPv6 Address: ff00::1

At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the static MVR6 groups assigned to an interface:

1. Click Multicast, MVR6.
2. Select Configure Static Group Member from the Step list.
3. Select Show from the Action list.
4. Select an MVR6 domain.
5. Select the port or trunk for which to display this information.

Figure 364: Showing the Static MVR6 Groups Assigned to a Port

The screenshot shows the 'Multicast > MVR6' configuration page. The 'Step' dropdown is set to '6. Configure Static Group Member' and the 'Action' dropdown is set to 'Show'. The configuration fields are as follows:

- Domain ID: 1
- Interface: Port 2 (selected), Trunk (unselected)

Below the configuration fields, there is a table titled 'MVR6 Static Group Member List' with a 'Total: 1' indicator. The table has two columns: 'VLAN' and 'Group IPv6 Address'.

VLAN	Group IPv6 Address
2	FF00::1

At the bottom right, there are 'Delete' and 'Revert' buttons.

DISPLAYING MVR6 RECEIVER GROUPS Use the Multicast > MVR6 (Show Member) page to show the multicast groups either statically or dynamically assigned to the MVR6 receiver groups on each interface.

CLI REFERENCES

- ◆ ["show mvr6 members" on page 1264](#)

PARAMETERS

These parameters are displayed:

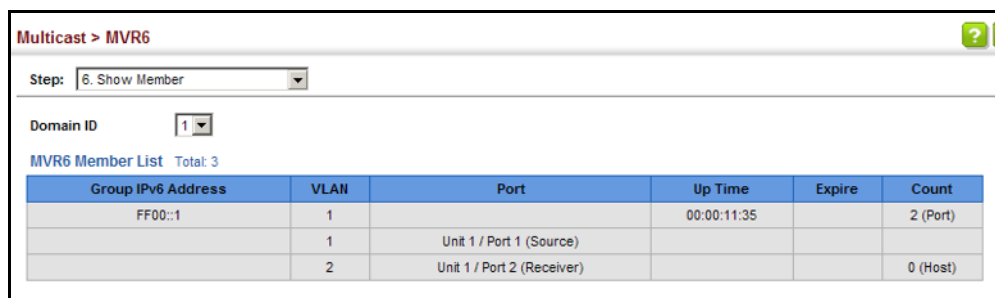
- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Group IPv6 Address** – Multicast groups assigned to the MVR6 VLAN.
- ◆ **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR6 VLAN if the group address has been statically assigned.
- ◆ **Port** – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned (these entries are marked as "Source"). Also shows the interfaces with subscribers for multicast services provided through the MVR6 VLAN (these entries are marked as "Receiver").
- ◆ **Up Time** – Time this service has been forwarded to attached clients.
- ◆ **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- ◆ **Count** – The number of multicast services currently being forwarded from the MVR6 VLAN.

WEB INTERFACE

To display the interfaces assigned to the MVR6 receiver groups:

1. Click Multicast, MVR6.
2. Select Show Member from the Step list.
3. Select an MVR6 domain.

Figure 365: Displaying MVR6 Receiver Groups



Group IPv6 Address	VLAN	Port	Up Time	Expire	Count
FF00::1	1		00:00:11:35		2 (Port)
	1	Unit 1 / Port 1 (Source)			
	2	Unit 1 / Port 2 (Receiver)			0 (Host)

DISPLAYING MVR6 STATISTICS Use the Multicast > MVR6 > Show Statistics pages to display MVR6 protocol-related statistics for the specified interface.

CLI REFERENCES

- ◆ ["show mvr6 statistics" on page 1266](#)

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28/52)
- ◆ **Trunk** – Trunk identifier. (Range: 1-16)

Query Statistics

- ◆ **Querier IPv6 Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **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.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **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 MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- ◆ **Report** – The number of MLD 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.

WEB INTERFACE

To display statistics for MVR6 query-related messages:

1. Click Multicast, MVR6.
2. Select Show Statistics from the Step list.
3. Select Show Query Statistics from the Action list.
4. Select an MVR6 domain.

Figure 366: Displaying MVR6 Statistics – Query

The screenshot shows the 'Multicast > MVR6' web interface. At the top, there are two dropdown menus: 'Step' set to '7. Show Statistics' and 'Action' set to 'Show Query Statistics'. Below these is a 'Domain ID' dropdown menu with '1' selected. The main section is titled 'Query Statistics' and contains a table with the following data:

Querier IPv6 Address	::
Querier Expire Time	00(h):00(m):00(s)
General Query Received	0
General Query Sent	34
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	0
Number of Leaves Sent	0

At the bottom left, there is a 'Clear All' button with a tooltip that says 'Click this button to clear all MVR6 statistics of the domain.' At the bottom right, there is a 'Refresh' button.

To display MVR6 protocol-related statistics for a VLAN:

1. Click Multicast, MVR6.
2. Select Show Statistics from the Step list.
3. Select Show VLAN Statistics from the Action list.
4. Select an MVR6 domain.
5. Select a VLAN.

Figure 367: Displaying MVR6 Statistics – VLAN

Multicast > MVR6

Step: 7. Show Statistics

Action: Show VLAN Statistics

Domain ID1

VLAN1

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	1
G(-S)-S Query	0		

Output Statistics

Report	0
Done	0
G Query	35
G(-S)-S Query	0

Clear

Refresh

To display MVR6 protocol-related statistics for a port:

1. Click Multicast, MVR6.
2. Select Show Statistics from the Step list.
3. Select Show Port Statistics from the Action list.
4. Select an MVR6 domain.
5. Select a Port.

Figure 368: Displaying MVR6 Statistics – Port

Multicast > MVR6

Step: 7. Show Statistics Action: Show Port Statistics

Domain ID 1

Port 1

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	12
Done	1
G Query	0
G(-S)-S Query	0

Clear Refresh

This chapter describes how to configure an initial IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. 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. An IPv6 global unicast or link-local address can be manually configured, or a link-local address can be dynamically generated.

This chapter provides information on network functions including:

- ◆ [IPv4 Configuration](#) – Sets an IPv4 address for management access.
- ◆ [IPv6 Configuration](#) – Sets an IPv6 address for management access.

SETTING THE SWITCH'S IP ADDRESS (IP VERSION 4)

Use the IP > General > Routing Interface (Add Address) page to configure an IPv4 address for the switch. An IPv4 address is obtained via DHCP by default for VLAN 1. To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment (if no routing protocols are enabled).

You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

CLI REFERENCES

- ◆ ["Basic IPv4 Configuration" on page 1368](#)
- ◆ ["DHCP Client" on page 1357](#)

COMMAND USAGE

- ◆ This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces, set up an IP interface for each VLAN.
- ◆ Once an IP address has been assigned to an interface, routing between different interfaces on the switch is enabled.

- ◆ To enable routing between interfaces defined on this switch and external network interfaces, you must configure static routes ([page 667](#)) or use dynamic routing; i.e., RIP ([page 672](#)).
- ◆ The precedence for configuring IP interfaces is the IP > General > Routing Interface (Add) menu, static routes ([page 667](#)), and then dynamic routing.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- ◆ **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)

- ◆ **IP Address Type** – Specifies a primary or secondary IP address. 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. For initial configuration, set this parameter to Primary. (Options: Primary, Secondary; Default: Primary)

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 in a network segment uses a secondary address, all other routers in that segment must also use a secondary address from the same network or subnet address space.

- ◆ **IP Address** – IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)



NOTE: You can manage the switch through any configured IP interface.

- ◆ **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.
- ◆ **Restart DHCP** – Requests a new IP address from the DHCP server for all enabled VLANs.

WEB INTERFACE

To set a static address for the switch:

1. Click IP, General, Routing Interface.
2. Select Add Address from the Action list.
3. Select any configured VLAN, set IP Address Mode to "Static," set IP Address Type to "Primary" if no address has yet been configured for this interface, and then enter the IP address and subnet mask.
4. Click Apply.

Figure 369: Configuring a Static IPv4 Address

The screenshot shows the 'IP > General > Routing Interface' configuration page. The 'Action' dropdown is set to 'Add Address'. The 'VLAN' dropdown is set to '1'. The 'IP Address Mode' dropdown is set to 'User Specified'. The 'IP Address Type' dropdown is set to 'Primary'. The 'IP Address' text field contains '192.168.0.2' and the 'Subnet Mask' text field contains '255.255.255.0'. Below these fields is a 'Restart DHCP' button and a link that says 'Click this button to restart DHCP service.' At the bottom right are 'Apply' and 'Revert' buttons.

To obtain an dynamic address through DHCP/BOOTP for the switch:

1. Click IP, General, Routing Interface.
2. Select Add Address from the Action list.
3. Select any configured VLAN, and set IP Address Mode to "BOOTP" or "DHCP."
4. Click Apply to save your changes.

IP will be enabled but will not function until a BOOTP or DHCP reply is received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server.

Figure 370: Configuring a Dynamic IPv4 Address

IP > General > Routing Interface

Action: Add Address

VLAN: 1

IP Address Mode: DHCP

IP Address Type: Primary

IP Address:

Subnet Mask:

Restart DHCP [Click this button to restart DHCP service.](#)

Apply Revert



NOTE: The switch will also broadcast a request for IP configuration settings on each power reset.

NOTE: If you lose the management connection, make a console connection to the switch and enter "show ip interface" to determine the new switch address.

Renewing DHCP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

To show the address configured for an interface:

1. Click IP, General, Routing Interface.
2. Select Add from the Action list.
3. Select an entry from the VLAN list.

Figure 371: Showing the Configured IP Address for an Interface

IP > General > Routing Interface

Action:

VLAN:

IP Address Mode: User Specified

Routing Interface IP List Total: 1

	IP Address Type	IP Address	Subnet Mask
<input type="checkbox"/>	Primary	192.168.0.2	255.255.255.0

SETTING THE SWITCH'S IP ADDRESS (IP VERSION 6)

This section describes how to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv4 address, see ["Setting the Switch's IP Address \(IP Version 4\)" on page 617](#).

COMMAND USAGE

- ◆ IPv6 includes two distinct address types – link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address.
- ◆ An IPv6 global unicast or link-local address can be manually configured (using the Add IPv6 Address page), or a link-local address can be dynamically generated (using the Configure Interface page).

CONFIGURING THE IPv6 DEFAULT GATEWAY

Use the IP > IPv6 Configuration (Configure Global) page to configure an IPv6 default gateway for the switch.

CLI REFERENCES

- ◆ ["ipv6 default-gateway" on page 1379](#)

PARAMETERS

These parameters are displayed:

- ◆ **Default Gateway** – Sets the IPv6 address of the default next hop router to use when no routing information is known about an IPv6 address.
 - If no routing protocol is enabled or static route defined, you must define a gateway if the target device is located in a different subnet.

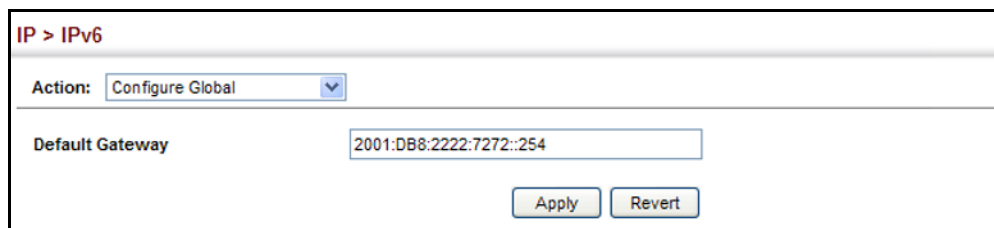
- If a routing protocol is enabled ([page 671](#)), you can still define a static route ([page 667](#)) to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
- An IPv6 address must be configured 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.

WEB INTERFACE

To configure an IPv6 default gateway for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Global from the Action list.
3. Enter the IPv6 default gateway.
4. Click Apply.

Figure 372: Configuring the IPv6 Default Gateway



The screenshot shows a web interface for configuring IPv6 settings. At the top, it says "IP > IPv6". Below that, there is a dropdown menu labeled "Action:" with "Configure Global" selected. Underneath, there is a field labeled "Default Gateway" with the value "2001:DB8:2222:7272::254" entered. At the bottom right, there are two buttons: "Apply" and "Revert".

CONFIGURING IPv6 INTERFACE SETTINGS

Use the IP > IPv6 Configuration (Configure Interface) page to configure general IPv6 settings for the selected VLAN, including explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.

CLI REFERENCES

- ◆ "IPv6 Interface" on [page 1378](#)

COMMAND USAGE

- ◆ The switch must be configured with a link-local address. The option to explicitly enable IPv6 creates a link-local address, but will not generate a global IPv6 address. The global unicast address must be manually configured (see ["Configuring an IPv6 Address" on page 627](#)).
- ◆ The option to explicitly enable IPv6 will also create a link-local address, but will not generate a global IPv6 address if auto-configuration is not

enabled. In this case, you must be manually configure an address (see ["Configuring an IPv6 Address" on page 627](#)).

- ◆ IPv6 Neighbor Discovery Protocol supersedes IPv4 Address Resolution Protocol in IPv6 networks. IPv6 nodes on the same network segment use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The key parameters used to facilitate this process are the number of attempts made to verify whether or not a duplicate address exists on the same network segment, and the interval between neighbor solicitations used to verify reachability information.

PARAMETERS

These parameters are displayed:

VLAN Mode

- ◆ **VLAN** – ID of a configured VLAN which is to be used for management access, or as a standard interface for a subnet. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)
- ◆ **Address Autoconfig** – Enables stateless autoconfiguration of an IPv6 address on an interface and enables IPv6 functionality on that interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address).
 - If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway).
 - If auto-configuration is not selected, then an address must be manually configured using the Add IPv6 Address page described below.
- ◆ **Enable IPv6 Explicitly** – Enables IPv6 on an interface and assigns it a link-local address. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled)

Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.
- ◆ **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes; Default: 1500 bytes)
 - The maximum value set in this field cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
 - If a non-default value is configured, an MTU option is included in the router advertisements sent from this device. This option is provided

to ensure that all nodes on a link use the same MTU value in cases where the link MTU is not otherwise well known.

- 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. If an IPv6 address has not been assigned to the switch, "N/A" is displayed in the MTU field.

◆ **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 3)

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended (see ["Configuring VLAN Groups" on page 196](#)). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

◆ **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds)

Default: 1000 milliseconds is used for neighbor discovery operations, 0 milliseconds is advertised in router advertisements.

This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the

reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.

- ◆ **ND Reachable-Time** – The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. (Range: 0-3600000 milliseconds)

Default: 30000 milliseconds is used for neighbor discovery operations, 0 milliseconds is advertised in router advertisements.

- The time limit configured by this parameter allows the router to detect unavailable neighbors.
- This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.
- Setting the time limit to 0 means that the configured time is unspecified by this router.

- ◆ **Restart DHCPv6** – 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) 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 Address Autoconfig option. 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 autoconfiguration, 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 autoconfiguration, in which a DHCPv6 server does not assign stateful addresses to IPv6 hosts, but does assign stateless configuration settings.

RA Mode

- ◆ **Interface** – Shows port or trunk configuration page.

- ◆ **RA Guard** – Blocks incoming Router Advertisement and Router Redirect packets. (Default: Disabled)

IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, note that unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.

RA Guard can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

WEB INTERFACE

To configure general IPv6 settings for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Select VLAN mode.
4. Specify the VLAN to configure.
5. Select Enable IPv6 Explicitly to automatically configure a link-local address and enable IPv6 on the selected interface. (To manually configure the link-local address, use the Add IPv6 Address page.) Set the MTU size, the maximum number of duplicate address detection messages, the neighbor solicitation message interval, and the amount of time that a remote IPv6 node is considered reachable.
6. Click Apply.

Figure 373: Configuring General Settings for an IPv6 Interface

The screenshot displays the 'IP > IPv6 Configuration' web interface. At the top, the 'Action' dropdown is set to 'Configure Interface'. Below this, the 'Mode' section has two radio buttons: 'VLAN' (selected) and 'RA Guard'. The 'VLAN' section shows a dropdown menu with '1' selected. The 'Address Autoconfig' section has a checkbox labeled 'Enabled' which is unchecked. The 'Enable IPv6 Explicitly' section also has a checkbox labeled 'Enabled' which is unchecked. The 'MTU (1280-65535)' section has a text input field with '1500' and the unit 'bytes'. The 'ND DAD Attempts (0-600)' section has a text input field with '3'. The 'ND NS Interval (1000-3600000)' section has a text input field with '1000' and the unit 'ms'. The 'ND Reachable-Time (0-3600000)' section has a text input field with '30000' and the unit 'ms'. At the bottom left, there is a 'Restart DHCPv6' button and a link that says 'Click this button to restart DHCPv6 service.' At the bottom right, there are 'Apply' and 'Revert' buttons.

To configure RA Guard for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Select RA Guard mode.
4. Enable RA Guard for untrusted interfaces.
5. Click Apply.

Figure 374: Configuring RA Guard for an IPv6 Interface

IP > IPv6 Configuration

Action: Configure interface

Mode: ☐ VLAN ☒ RA Guard

Interface: ☒ Port ☐ Trunk

Port List Total: 28

Port	RA Guard
1	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled

CONFIGURING AN IPv6 ADDRESS

Use the IP > IPv6 Configuration (Add IPv6 Address) page to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets.

CLI REFERENCES

- ◆ ["IPv6 Interface" on page 1378](#)

COMMAND USAGE

- ◆ All IPv6 addresses 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 must always be configured with a link-local address. Therefore, explicitly enabling IPv6 (see ["Configuring IPv6 Interface Settings" on page 622](#)) or manually assigning a global unicast address will also automatically generate a link-local unicast address. The prefix length for a link-local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). Alternatively, you can manually configure the link-local address by entering the full address with a network prefix in the range of FE80~FEBF.

- ◆ To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:
 - It can be manually configured by specifying the entire network prefix and prefix length, and using the EUI-64 form of the interface identifier to automatically create the low-order 64 bits in the host portion of the address.
 - You can also manually configure the global unicast address by entering the full address and prefix length.
- ◆ You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- ◆ If a duplicate link-local address is detected on the local segment, this interface is disabled and a warning message displayed on the console. If a duplicate global unicast address is detected on the network, the address is disabled on this interface and a warning message displayed on the console.
- ◆ When an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of a configured VLAN which is to be used for management access, or for creating an interface to multiple subnets. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)
- ◆ **Address Type** – Defines the address type configured for this interface.
 - **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and 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).
 - **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.
 - When using EUI-64 format for the low-order 64 bits in the host portion of the address, the value entered in the IPv6 Address field includes the network portion of the address, and the prefix length indicates how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address). Note that the value specified in the IPv6 Address field 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 bits used in the network portion of the address will take precedence over the interface identifier.

- 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., organizationally unique identifier, or company identifier) 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.

- **Link Local** – Configures an IPv6 link-local address.
 - The address prefix must be in the range of FE80~FEBF.
 - You can configure only one link-local address per interface.
 - The specified address replaces a link-local address that was automatically generated for the interface.

◆ **IPv6 Address** – IPv6 address assigned to this interface.

WEB INTERFACE

To configure an IPv6 address:

1. Click IP, IPv6 Configuration.
2. Select Add IPv6 Address from the Action list.
3. Specify the VLAN to configure, select the address type, and then enter an IPv6 address and prefix length.
4. Click Apply.

Figure 375: Configuring an IPv6 Address

The screenshot shows a web-based configuration interface for IPv6. At the top, it says 'IP > IPv6'. Below that, there's a section for 'Action:' with a dropdown menu set to 'Add IPv6 Address'. Underneath, there are three fields: 'VLAN' with a dropdown set to '1', 'Address Type' with a dropdown set to 'Global', and 'IPv6 Address' with a text box containing '2001:DB8:2222:7272::72/96'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

SHOWING IPv6 ADDRESSES Use the IP > IPv6 Configuration (Show IPv6 Address) page to display the IPv6 addresses assigned to an interface.

CLI REFERENCES

- ◆ ["show ipv6 interface" on page 1388](#)

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of a configured VLAN which is to be used for management access, or for creating an interface to multiple subnets. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)
- ◆ **IPv6 Address Type** – The address type (Global, EUI-64, Link Local).
- ◆ **IPv6 Address** – An IPv6 address assigned to this interface.

In addition to the unicast addresses assigned to an interface, a node is also required to listen to the all-nodes multicast addresses FF01::1 (interface-local scope) and FF02::1 (link-local scope).

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.

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.

Note that the solicited-node multicast address (link-local scope FF02) is used to resolve the MAC addresses for neighbor nodes since IPv6 does not support the broadcast method used by the Address Resolution Protocol in IPv4.

These additional addresses are displayed by the CLI (see ["show ip interface" on page 1371](#)).

- ◆ **Configuration Mode** – Indicates if this address was automatically generated or manually configured.

WEB INTERFACE

To show the configured IPv6 addresses:

1. Click IP, IPv6 Configuration.
2. Select Show IPv6 Address from the Action list.
3. Select a VLAN from the list.

Figure 376: Showing Configured IPv6 Addresses

The screenshot shows the 'IP > IPv6 Configuration' web interface. At the top, there is a breadcrumb 'IP > IPv6 Configuration' and a help icon. Below this is an 'Action:' dropdown menu set to 'Show IPv6 Address'. Underneath is a 'VLAN' dropdown menu set to '1'. The main section is titled 'IPv6 Address List Total: 2'. It contains a table with the following data:

<input type="checkbox"/>	IPv6 Address Type	IPv6 Address	Configuration Mode
<input type="checkbox"/>	Global	2001:db8:2222:7272::72/96[INVALID]	Manual
<input type="checkbox"/>	Link Local	fe80::200:e8ff:fe94:4000%1/64	Auto

At the bottom of the table are 'Delete' and 'Revert' buttons.

SHOWING THE IPv6 NEIGHBOR CACHE

Use the IP > IPv6 Configuration (Show IPv6 Neighbor Cache) page to display the IPv6 addresses detected for neighbor devices.

CLI REFERENCES

- ◆ ["show ipv6 neighbors" on page 1404](#)

PARAMETERS

These parameters are displayed:

Table 37: ShowIPv6 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 Address	Physical layer MAC address.

Table 37: ShowIPv6 Neighbors - display description (Continued)

Field	Description
State	<p>The following states are used for dynamic entries:</p> <ul style="list-style-type: none"> ◆ 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. ◆ Invalid - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293). ◆ Reachable - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in Reachable state, the device takes no special action when sending packets. ◆ 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. ◆ 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. ◆ Probe - A reachability confirmation is actively sought by re-sending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received. ◆ Unknown - Unknown state. <p>The following states are used for static entries:</p> <ul style="list-style-type: none"> ◆ Incomplete - The interface for this entry is down. ◆ Permanent - Indicates a static entry. ◆ Reachable - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
VLAN	VLAN interface from which the address was reached.

WEB INTERFACE

To show neighboring IPv6 devices:

1. Click IP, IPv6 Configuration.
2. Select Show IPv6 Neighbors from the Action list.

Figure 377: Showing IPv6 Neighbors

The screenshot shows the 'IP > IPv6 Configuration' page. Under the 'Action:' dropdown, 'Show IPv6 Neighbor Cache' is selected. Below this, the 'Current Neighbor Cache Table' is displayed with a 'Total: 1' count. The table has five columns: IPv6 Address, Age, Link-layer Address, State, and VLAN. It contains one entry with the IPv6 address 2001:DB8:2222:7272::74, an age of 20, a link-layer address of 00-E0-0C-9C-CA-10, a state of 'Reachable', and a VLAN of 1. A 'Clear' button is located at the bottom right of the table area.

IPv6 Address	Age	Link-layer Address	State	VLAN
2001:DB8:2222:7272::74	20	00-E0-0C-9C-CA-10	Reachable	1

SHOWING IPV6 STATISTICS Use the IP > IPv6 Configuration (Show Statistics) page to display statistics about IPv6 traffic passing through this switch.

CLI REFERENCES

- ◆ "show ipv6 traffic" on page 1391

COMMAND USAGE

This switch provides statistics for the following traffic types:

- ◆ **IPv6** – The Internet Protocol for Version 6 addresses provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (that is, hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.
- ◆ **ICMPv6** – Internet Control Message Protocol for Version 6 addresses is a network layer protocol that transmits message packets to report errors in processing IPv6 packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (that is, the next hop router) to use for a specific destination.
- ◆ **UDP** – User Datagram Protocol provides a datagram mode of packet switched communications. It uses IP as the underlying transport mechanism, providing 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.

PARAMETERS

These parameters are displayed:

Table 38: Show IPv6 Statistics - display description

Field	Description
IPv6 Statistics	
<i>IPv6 Received</i>	
Total	The total number of input datagrams received by the interface, including those received in error.
Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
Too Big Errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.

Table 38: Show IPv6 Statistics - display description (Continued)

Field	Description
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.
Reassembly Request Datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Reassembled 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.
Reassembled 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 Transmitted</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 ipv6IfStatsOutForwDatagrams.
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 ipv6IfStatsOutForwDatagrams 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.

Table 38: Show IPv6 Statistics - display description (Continued)

Field	Description
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.
ICMPv6 Statistics	
<i>ICMPv6 received</i>	
Input	The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. 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 Messages	The number of ICMP Parameter Problem messages received by the interface.
Echo Request Messages	The number of ICMP Echo (request) messages received by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages received by the interface.
Router Solicit Messages	The number of ICMP Router Solicit messages received by the interface.
Router Advertisement Messages	The number of ICMP Router Advertisement messages received by the interface.
Neighbor Solicit Messages	The number of ICMP Neighbor Solicit messages received by the interface.
Neighbor Advertisement Messages	The number of ICMP Neighbor Advertisement messages received by the interface.
Redirect Messages	The number of Redirect messages received by the interface.
Group Membership Query Messages	The number of ICMPv6 Group Membership Query messages received by the interface.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages received by the interface.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Multicast Listener Discovery Version 2 Reports	The number of MLDv2 reports received by the interface.
<i>ICMPv6 Transmitted</i>	
Output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.

Table 38: Show IPv6 Statistics - display description (Continued)

Field	Description
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.
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.
UDP Statistics	
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.

WEB INTERFACE

To show the IPv6 statistics:

1. Click IP, IPv6 Configuration.
2. Select Show Statistics from the Action list.
3. Click IPv6, ICMPv6 or UDP.

Figure 378: Showing IPv6 Statistics (IPv6)

IP > IPv6

Action: Show Statistics

Type ☒ IPv6 ☐ ICMPv6 ☐ UDP

IPv6 Statistics

Total Received	55	Received Reassembled Succeeded
Received Header Errors	0	Received Reassembled Failed
Received Too Big Errors	0	Transmitted Forwards Datagrams
Received No Routes	0	Transmitted Requests
Received Address Errors	0	Transmitted Discards
Received Unknown Protocols	0	Transmitted No Routes
Received Truncated Packets	0	Transmitted Generated Fragments
Received Discards	0	Transmitted Fragment Succeeded
Received Delivers	55	Transmitted Fragment Failed
Received Reassembly Request Datagrams	0	

Clear

Figure 379: Showing IPv6 Statistics (ICMPv6)

IP > IPv6 Configuration

Action: Show Statistics

Type ☐ IPv6 ☒ ICMPv6 ☐ UDP

ICMPv6 Statistics

Received Input	0	Transmitted Output	0
Received Errors	0	Transmitted Destination Unreachable Messages	0
Received Destination Unreachable Messages	0	Transmitted Packet Too Big Messages	0
Received Packet Too Big Messages	0	Transmitted Time Exceeded Messages	0
Received Time Exceeded Messages	0	Transmitted Parameter Problem Message	0
Received Parameter Problem Messages	0	Transmitted Echo Request Messages	0
Received Echo Request Messages	0	Transmitted Echo Reply Messages	0
Received Echo Reply Messages	0	Transmitted Router Solicit Messages	0
Received Router Solicit Messages	0	Transmitted Router Advertisement Messages	0
Received Router Advertisement Messages	0	Transmitted Neighbor Solicit Messages	0
Received Neighbor Solicit Messages	0	Transmitted Neighbor Advertisement Messages	0
Received Neighbor Advertisement Messages	0	Transmitted Redirect Messages	0
Received Redirect Messages	0	Transmitted Group Membership Query Messages	0
Received Group Membership Query Messages	0	Transmitted Group Membership Response Messages	0
Received Group Membership Response Messages	0	Transmitted Group Membership Reduction Messages	0
Received Group Membership Reduction Messages	0	Transmitted Multicast Listener Discovery Version 2 Reports	0
Received Multicast Listener Discovery Version 2 Reports	0		

Clear

Figure 380: Showing IPv6 Statistics (UDP)

The screenshot shows the 'IP > IPv6' configuration page. At the top, there is a breadcrumb 'IP > IPv6'. Below it is an 'Action:' dropdown menu set to 'Show Statistics'. Underneath, there are three radio buttons for 'Type': 'IPv6', 'ICMPv6', and 'UDP'. The 'UDP' radio button is selected. Below the radio buttons, the section 'UDP Statistics' is displayed. It contains four rows of statistics: 'Input' with a value of 10, 'No Port Errors' with a value of 0, 'Other Errors' with a value of 0, and 'Output' with a value of 1. At the bottom right of the statistics section is a 'Clear' button.

SHOWING THE MTU FOR RESPONDING DESTINATIONS

Use the IP > IPv6 Configuration (Show MTU) page to display 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.

CLI REFERENCES

◆ ["show ipv6 mtu" on page 1390](#)

PARAMETERS

These parameters are displayed:

Table 39: Show 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.

WEB INTERFACE

To show the MTU reported from other devices:

1. Click IP, IPv6 Configuration.
2. Select Show MTU from the Action list.

Figure 381: Showing Reported MTU Values

The screenshot shows the 'IP > IPv6' configuration page with the 'Action:' dropdown set to 'Show MTU'. Below this, there is a section titled 'MTU Table Total: 2'. It contains a table with three columns: 'MTU', 'Since', and 'Destination Address'. The table has two rows of data.

MTU	Since	Destination Address
1400	00:04:21	5000:1::3
1280	00:04:50	FE80::203:A0FF:FED6:141D

This chapter describes how to configure Domain Name Service (DNS) on this switch. For information on DHCP snooping which is included in this folder, see ["DHCP Snooping" on page 402](#).

This chapter provides information on the following IP services, including:

- ◆ [DNS](#) – Configures default domain names, identifies servers to use for dynamic lookup, and shows how to configure static entries.
- ◆ [DHCP Client](#) – Specifies the DHCP client identifier for an interface.
- ◆ [DHCP Relay](#) – Enables DHCP relay service, and defines the servers to which client requests are forwarded.
- ◆ [PPPoE Intermediate Agent](#) – Configures PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

DOMAIN NAME SERVICE

DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

CONFIGURING GENERAL DNS SERVICE PARAMETERS

Use the IP Service > DNS - General (Configure Global) page to enable domain lookup and set the default domain name.

CLI REFERENCES

- ◆ ["ip domain-lookup" on page 1348](#)
- ◆ ["ip domain-name" on page 1349](#)

COMMAND USAGE

- ◆ To enable DNS service on this switch, enable domain lookup status, and configure one or more name servers (see ["Configuring a List of Name Servers" on page 642](#)).

PARAMETERS

These parameters are displayed:

- ◆ **Domain Lookup** – Enables DNS host name-to-address translation.
(Default: Disabled)
- ◆ **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-127 alphanumeric characters)

WEB INTERFACE

To configure general settings for DNS:

1. Click IP Service, DNS.
2. Select Configure Global from the Action list.
3. Enable domain lookup, and set the default domain name.
4. Click Apply.

Figure 382: Configuring General Settings for DNS

IP Service > DNS > General

Action: Configure Global

Domain Lookup ☒ Enabled

Default Domain Name

Apply Revert

CONFIGURING A LIST OF DOMAIN NAMES

Use the IP Service > DNS - General (Add Domain Name) page to configure a list of domain names to be tried in sequential order.

CLI REFERENCES

- ◆ ["ip domain-list" on page 1347](#)
- ◆ ["show dns" on page 1353](#)

COMMAND USAGE

- ◆ Use this page to define 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).
- ◆ If there is no domain list, the default domain name is used (see ["Configuring General DNS Service Parameters" on page 639](#)). If there is a domain list, the system will search it for a corresponding entry. If none is found, it will use the default domain name.
- ◆ When an incomplete host name is received by the DNS service on this switch and a domain name list has been specified, the switch 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 (see ["Configuring a List of Name Servers" on page 642](#)).

PARAMETERS

These parameters are displayed:

Domain Name – Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-68 characters)

WEB INTERFACE

To create a list domain names:

1. Click IP Service, DNS.
2. Select Add Domain Name from the Action list.
3. Enter one domain name at a time.
4. Click Apply.

Figure 383: Configuring a List of Domain Names for DNS

The screenshot shows the 'IP Service > DNS > General' configuration page. The 'Action:' dropdown menu is set to 'Add Domain Name'. Below it, the 'Domain Name' text input field contains the value 'sample.com.uk'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the list domain names:

1. Click IP Service, DNS.
2. Select Show Domain Names from the Action list.

Figure 384: Showing the List of Domain Names for DNS

The screenshot shows the 'IP Service > DNS > General' configuration page. The 'Action:' dropdown menu is set to 'Show Domain Names'. Below it, there is a table titled 'Domain Name List' with a 'Total: 2' indicator. The table has two columns: a checkbox column and a 'Domain Name' column. The first row shows a checked checkbox and the domain 'google.com'. The second row shows an unchecked checkbox and the domain 'hinet.net'. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Domain Name
<input checked="" type="checkbox"/>	google.com
<input type="checkbox"/>	hinet.net

CONFIGURING A LIST OF NAME SERVERS Use the IP Service > DNS - General (Add Name Server) page to configure a list of name servers to be tried in sequential order.

CLI REFERENCES

- ◆ "ip name-server" on page 1351
- ◆ "show dns" on page 1353

COMMAND USAGE

- ◆ To enable DNS service on this switch, configure one or more name servers, and enable domain lookup status (see ["Configuring General DNS Service Parameters" on page 639](#)).
- ◆ When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- ◆ If all name servers are deleted, DNS will automatically be disabled. This is done by disabling the domain lookup status.

PARAMETERS

These parameters are displayed:

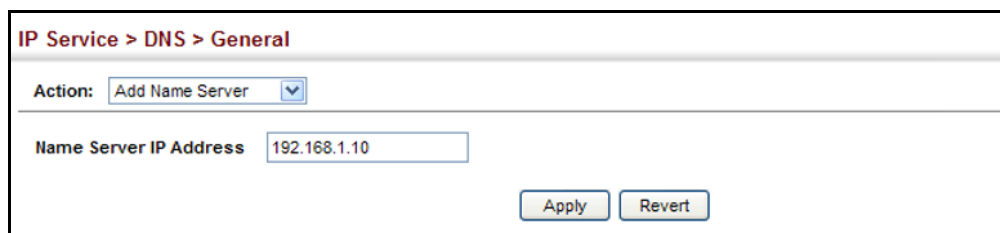
Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

WEB INTERFACE

To create a list name servers:

1. Click IP Service, DNS.
2. Select Add Name Server from the Action list.
3. Enter one name server at a time.
4. Click Apply.

Figure 385: Configuring a List of Name Servers for DNS



The screenshot shows a web interface for configuring DNS. At the top, the breadcrumb is "IP Service > DNS > General". Below this, there is a section titled "Action:" with a dropdown menu currently set to "Add Name Server". Underneath, there is a label "Name Server IP Address" followed by a text input field containing the IP address "192.168.1.10". At the bottom right of the form, there are two buttons: "Apply" and "Revert".

To show the list name servers:

1. Click IP Service, DNS.
2. Select Show Name Servers from the Action list.

Figure 386: Showing the List of Name Servers for DNS

IP Service > DNS > General

Action: Show Name Servers

Name Server IP Address List Total: 3

<input type="checkbox"/>	Name Server IP Address
<input type="checkbox"/>	192.168.1.10
<input type="checkbox"/>	140.113.5.7
<input type="checkbox"/>	10.7.231.5

Delete Revert

CONFIGURING STATIC DNS HOST TO ADDRESS ENTRIES

Use the IP Service > DNS - Static Host Table (Add) page to manually configure static entries in the DNS table that are used to map domain names to IP addresses.

CLI REFERENCES

- ◆ ["ip host" on page 1350](#)
- ◆ ["show hosts" on page 1354](#)

COMMAND USAGE

- ◆ Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.

PARAMETERS

These parameters are displayed:

- ◆ **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)
- ◆ **IP Address** – IPv4 or IPv6 address(es) associated with a host name.

WEB INTERFACE

To configure static entries in the DNS table:

1. Click IP Service, DNS, Static Host Table.
2. Select Add from the Action list.
3. Enter a host name and the corresponding address.
4. Click Apply.

Figure 387: Configuring Static Entries in the DNS Table

IP Service > DNS > Static Host Table

Action:

Add

Host Name

yahoo.com

IP Address

10.2.78.3

Apply

Revert

To show static entries in the DNS table:

1. Click IP Service, DNS, Static Host Table.
2. Select Show from the Action list.

Figure 388: Showing Static Entries in the DNS Table

IP Service > DNS > Static Host Table

Action:

Show

IP Address List

Total: 3

	Host	IP Address
<input type="checkbox"/>	yahoo.com	10.2.78.3
<input type="checkbox"/>	hinet.net	124.29.31.155
<input type="checkbox"/>	google.com	133.45.211.18

Delete

Revert

DISPLAYING THE DNS CACHE Use the IP Service > DNS - Cache page to display entries in the DNS cache that have been learned via the designated name servers.

CLI REFERENCES

- ◆ ["show dns cache" on page 1354](#)

COMMAND USAGE

- ◆ Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

PARAMETERS

These parameters are displayed:

- ◆ **No.** – The entry number for each resource record.
- ◆ **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.

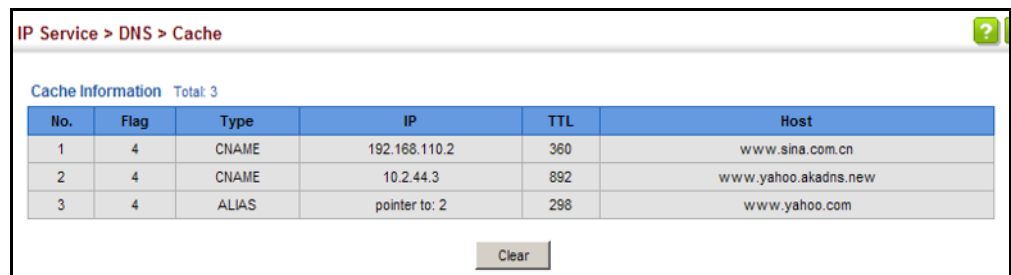
- ◆ **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- ◆ **IP** – The IP address associated with this record.
- ◆ **TTL** – The time to live reported by the name server.
- ◆ **Host** – The host name associated with this record.

WEB INTERFACE

To display entries in the DNS cache:

1. Click IP Service, DNS, Cache.

Figure 389: Showing Entries in the DNS Cache



The screenshot shows a web interface titled "IP Service > DNS > Cache". Below the title, it says "Cache Information Total: 3". There is a table with 6 columns: No., Flag, Type, IP, TTL, and Host. The table contains 3 rows of data. Below the table is a "Clear" button.

No.	Flag	Type	IP	TTL	Host
1	4	CNAME	192.168.110.2	360	www.sina.com.cn
2	4	CNAME	10.2.44.3	892	www.yahoo.akadns.net
3	4	ALIAS	pointer to: 2	298	www.yahoo.com

DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet.

SPECIFYING A DHCP CLIENT IDENTIFIER

Use the IP Service > DHCP > Client page to specify the DHCP client identifier for a VLAN interface.

CLI REFERENCES

- ◆ ["ip dhcp client class-id" on page 1358](#)

COMMAND USAGE

- ◆ The class identifier is used 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 40: 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" 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 41: 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 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.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **VLAN** – ID of configured VLAN.
- ◆ **Vendor Class ID** – The following options are supported when the check box is marked to enable this feature:
 - **Default** – The default string is ECS4510-28T, ECS4510-28F, ECS4510-28P, ECS4510-52T, or ECS4510-52P.
 - **Text** – A text string. (Range: 1-32 characters)
 - **Hex** – A hexadecimal value. (Range: 1-64 characters)

WEB INTERFACE

To configure a DHCP client identifier:

1. Click IP Service, DHCP, Client.
2. Mark the check box to enable this feature. Select the default setting, or the format for a vendor class identifier. If a non-default value is used, enter a text string or hexadecimal value.
3. Click Apply.

Figure 390: Specifying A DHCP Client Identifier

IP Service > DHCP > Client

VLAN: 1

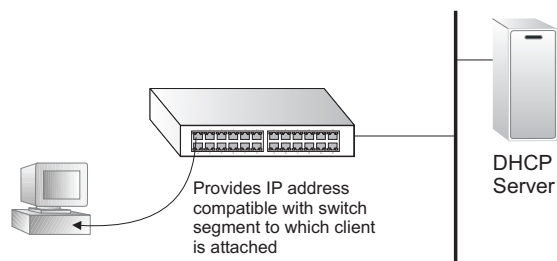
Vendor Class ID: ☒ Default

Apply Revert

CONFIGURING DHCP RELAY SERVICE

Use the IP Service > DHCP > Relay page to configure DHCP relay service for attached host devices. If DHCP relay is enabled, and this switch sees a DHCP request broadcast, 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 the DHCP server. 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.

Figure 391: Layer 3 DHCP Relay Service



CLI REFERENCES

- ◆ ["ip dhcp relay server" on page 1364](#)
- ◆ ["ip dhcp restart relay" on page 1365](#)

COMMAND USAGE

- ◆ You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.

- ◆ DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN ID** – ID of configured VLAN.
- ◆ **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.
- ◆ **Restart DHCP Relay** – Use this button to re-initialize DHCP relay service.

WEB INTERFACE

To configure DHCP relay service:

1. Click IP Service, DHCP, Relay.
2. Enter up to five IP addresses for any VLAN.
3. Click Apply.

Figure 392: Configuring DHCP Relay Service

IP Service > DHCP > Relay

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

DHCP Server by VLAN List Total: 1

VLAN	Server IP Address
1	192.168.2.33 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0

Restart DHCP Relay Click the button to restart DHCP Relay service.

Apply Revert

CONFIGURING THE PPPoE INTERMEDIATE AGENT

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

CONFIGURING PPPoE IA GLOBAL SETTINGS

Use the IP Service > PPPoE Intermediate Agent (Configure Global) page to enable the PPPoE IA on the switch, set the access node identifier, and set the generic error message.

CLI REFERENCES

- ◆ "pppoe intermediate-agent" on page 879
- ◆ "pppoe intermediate-agent port-format-type" on page 881
- ◆ "show pppoe intermediate-agent info" on page 884

COMMAND USAGE

When PPPoE IA is enabled, the switch inserts a tag identifying itself as a PPPoE IA 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 on the Configure Interface page). 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.

PARAMETERS

These parameters are displayed:

- ◆ **PPPoE IA Global Status** – Enables the PPPoE Intermediate Agent globally on the switch. (Default: Disabled)

Note that PPPoE IA must be enabled globally before it can be enabled on an interface.
- ◆ **Access Node Identifier** – String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters; Default: IP address of first IPv4 interface on the switch.)

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 on the Configure Interface page.
- ◆ **Operational Access Node Identifier** – The configured access node identifier.
- ◆ **Generic Error Message** – An error message notifying the sender that the PPPoE Discovery packet was too large. (Range: 0-127; Default: PPPoE Discover packet too large to process. Try reducing the number of tags added.)
- ◆ **Operational Generic Error Message** – The configured generic error message.

WEB INTERFACE

To configure global settings for PPPoE IA:

1. Click IP Service, PPPoE Intermediate Agent.
2. Select Configure Global from the Step list.
3. Enable the PPPoE IA on the switch, set the access node identifier, and set the generic error message.
4. Click Apply.

Figure 393: Configuring Global Settings for PPPoE Intermediate Agent

IP Service > PPPoE Intermediate Agent

Step: 1. Configure Global

PPPoE IA Global Status ☐ Enabled

Access Node Identifier

Operational Access Node Identifier 10.254.254.1

Generic Error Message

Operational Generic Error Message PPPoE Discover packet too large to process. Try reducing the number of tags added.

Apply Revert

CONFIGURING PPPoE IA INTERFACE SETTINGS

Use the IP Service > PPPoE Intermediate Agent (Configure Interface) page to enable PPPoE IA on an interface, set trust status, enable vendor tag stripping, and set the circuit ID and remote ID.

CLI REFERENCES

- ◆ ["PPPoE Intermediate Agent" on page 879](#)

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or trunk selection.
- ◆ **PPPoE IA Status** – Enables the PPPoE IA on an interface. (Default: Disabled)

Note that PPPoE IA must also be enabled globally on the switch for this command to take effect.
- ◆ **Trust Status** – Sets an interface to trusted mode to indicate that it is connected to a PPPoE server. (Default: Disabled)
 - 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.
- ◆ **Vendor Tag Strip** – Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. (Default: Disabled)

This parameter 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.
- ◆ **Circuit ID** – String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters; Default: Unit/Port:VLAN-ID, or 0/Trunk-ID:VLAN-ID)
 - 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.

◆ **Operational Circuit ID** – The configured circuit identifier.

◆ **Remote ID** – String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters; Default: Port MAC address)

◆ **Operational Remote ID** – The configured circuit identifier.

WEB INTERFACE

To configure interface settings for PPPoE IA:

1. Click IP Service, PPPoE Intermediate Agent.
2. Select Configure Interface from the Step list.
3. Select Port or Trunk interface type.
4. Enable PPPoE IA on an interface, set trust status, enable vendor tag stripping if required, and set the circuit ID and remote ID.
5. Click Apply.

Figure 394: Configuring Interface Settings for PPPoE Intermediate Agent

IP Service > PPPoE Intermediate Agent

Step: 2. Configure Interface

Interface: ☒ Port ☐ Trunk

PPPoE Intermediate Agent Port List Total: 12

Port	PPPoE IA Status	Trust Status	Vendor Tag Strip	Circuit ID	Operation Circuit ID	Remote ID	Operation Remote ID
1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled		1/1:vid		00-E0-0C-00-00-FE
2	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled		1/2:vid		00-E0-0C-00-00-FF
3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled		1/3:vid		00-E0-0C-00-01-00
4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled		1/4:vid		00-E0-0C-00-01-01
5	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled		1/5:vid		00-E0-0C-00-01-02

SHOWING PPPoE IA STATISTICS Use the IP Service > PPPoE Intermediate Agent (Show Statistics) page to show statistics on PPPoE IA protocol messages.

CLI REFERENCES

- ◆ ["show pppoe intermediate-agent statistics" on page 885](#)

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or trunk selection.
- ◆ **Received** – Received PPPoE active discovery messages.
 - **All** – All PPPoE active discovery message types.
 - **PADI** – PPPoE Active Discovery Initiation messages.
 - **PADO** – PPPoE Active Discovery Offer messages.
 - **PADR** – PPPoE Active Discovery Request messages.
 - **PADS** – PPPoE Active Discovery Session-Confirmation messages.
 - **PADT** – PPPoE Active Discovery Terminate messages.
- ◆ **Dropped** – Dropped PPPoE active discovery messages.
 - **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.

WEB INTERFACE

To show statistics for PPPoE IA protocol messages:

1. Click IP Service, PPPoE Intermediate Agent.
2. Select Show Statistics from the Step list.
3. Select Port or Trunk interface type.

Figure 395: Showing PPPoE Intermediate Agent Statistics

IP Service > PPPoE Intermediate Agent										
Step: 3. Show Statistics										
Interface <input checked="" type="radio"/> Port <input type="radio"/> Trunk										
PPPoE Intermediate Agent Statistics Total: 12										
	Port	Received						Dropped		
		All	PADI	PADO	PADR	PADS	PADT	Response from untrusted	Request towards untrusted	Malformed
<input type="checkbox"/>	1	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	2	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0

This chapter provides information on network functions including:

- ◆ [Ping](#) – Sends ping message to another node on the network.
- ◆ [Trace](#) – Sends ICMP echo request packets to another node on the network.
- ◆ [Address Resolution Protocol](#) – Describes how to configure ARP aging time, proxy ARP, or static addresses. Also shows how to display dynamic entries in the ARP cache.
- ◆ [Static Routes](#) – Configures static routes to other network segments.
- ◆ [Routing Table](#) – Displays routing entries learned through dynamic routing and statically configured entries.

OVERVIEW

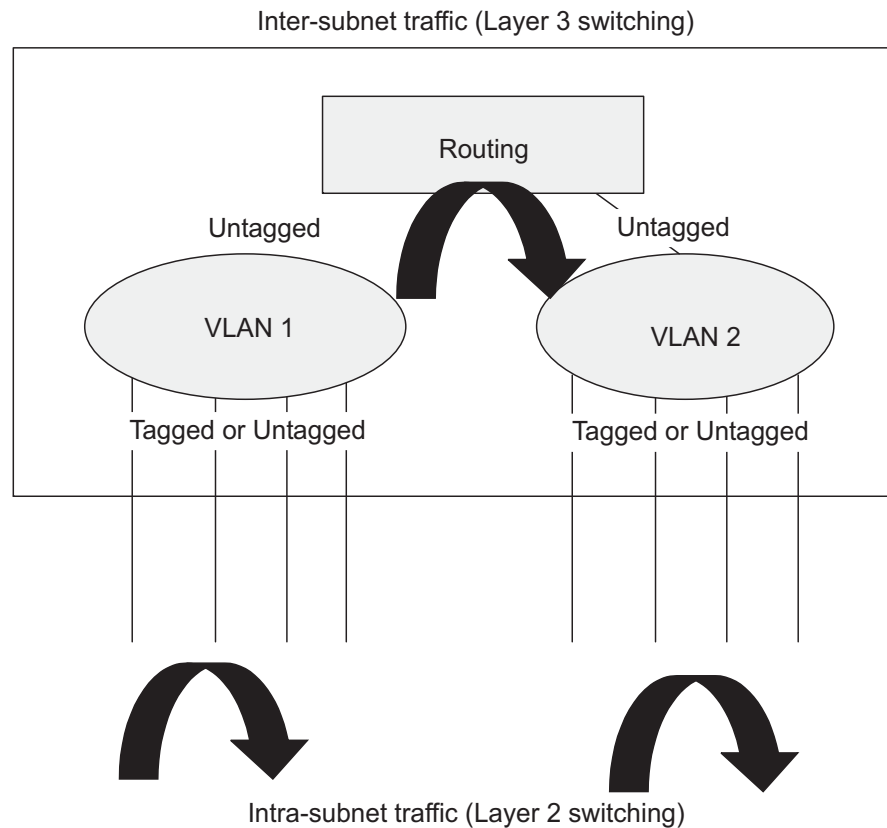
This switch supports IP routing and routing path management via static routing definitions ([page 1408](#)) and dynamic routing protocols such as RIP ([page 672](#)). When IP routing is functioning, this switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, default routing can only forward traffic between local IP interfaces. As with all traditional routers, static and dynamic routing functions must first be configured to work.

INITIAL CONFIGURATION

By default, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. To segment the attached network, first create VLANs for each unique user group or application traffic ([page 196](#)), assign all ports that belong to the same group to these VLANs ([page 199](#)), and then assign an IP interface to each VLAN ([page 617](#) or [page 621](#)). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.

Figure 396: Virtual Interfaces and Layer 3 Routing



IP ROUTING AND SWITCHING

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- ◆ Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- ◆ Layer 3 forwarding (routing):
 - Based on the Layer 3 destination address
 - Replacing destination/source MAC addresses for each hop
 - Incrementing the hop count
 - Decrementing the time-to-live
 - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is

broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to the next hop router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node through the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.



NOTE: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

ROUTING PATH MANAGEMENT

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- ◆ Handling routing protocols
- ◆ Updating the routing table
- ◆ Updating the Layer 3 switching database

ROUTING PROTOCOLS The switch supports both static and dynamic routing.

- ◆ Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- ◆ Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

CONFIGURING IP ROUTING INTERFACES

CONFIGURING LOCAL AND REMOTE INTERFACES Use the IP > General > Routing Interface (Configure Interface - Add Address) page to configure routing interfaces for directly connected IPv4 subnets (see ["Setting the Switch's IP Address \(IP Version 4\)" on page 617](#)). Or use the IP > IPv6 Configuration pages to configure routing interfaces for directly connected IPv6 subnets (see ["Setting the Switch's IP Address \(IP Version 6\)" on page 621](#)).

If this router is directly connected to end node devices (or connected to end nodes through shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network prefix number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network segment that is connected to that interface, and allows you to send IP packets to or from the router.

You can specify the IP subnets connected directly to this router by manually assigning an IP address to each VLAN, or using BOOTP or DHCP to dynamically assign an address. To specify IP subnets not directly connected to this router, you can either configure static routes (see [page 667](#)), or use the RIP dynamic routing protocol (see [page 671](#)) to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Once IP interfaces have been configured, the switch functions as a multilayer routing switch, operating at either Layer 2 or 3 as required. All IP packets are routed directly between local interfaces, or indirectly to remote interfaces using either static or dynamic routing. All other packets for non-IP protocols (for example, NetBuei, NetWare or AppleTalk) are switched based on MAC addresses).

To route traffic between remote IP interfaces, the switch should be recognized by other network nodes as an IP router, either by setting it to advertise itself as the default gateway or by redirection from another router via the ICMP process used by various routing protocols.

If the switch is configured to advertise itself as the default gateway, a routing protocol must still be used to determine the next hop router for any unknown destinations, i.e., packets that do not match any routing table entry. If another router is designated as the default gateway, then the switch will pass packets to this router for any unknown hosts or subnets.

To configure a default gateway for IPv4, use the static routing table as described on [page 1408](#), enter 0.0.0.0 for the IP address and subnet mask, and then specify this switch itself or another router as the gateway. To configure a gateway for IPv6, see ["Configuring the IPv6 Default Gateway" on page 621](#).

USING THE PING FUNCTION Use the IP > General > Ping page to send ICMP echo request packets to another node on the network.

CLI REFERENCES

- ◆ ["ping" on page 1373](#)

PARAMETERS

These parameters are displayed:

- ◆ **Host Name/IP Address** – IPv4/IPv6 address or alias of the host.
- ◆ **Probe Count** – Number of packets to send. (Range: 1-16)
- ◆ **Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes for IPv4, 0-1500 bytes for IPv6)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

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.
- ◆ 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.

WEB INTERFACE

To ping another device on the network:

1. Click IP, General, Ping.
2. Specify the target device and ping parameters.
3. Click Apply.

Figure 397: Pinging a Network Device

The screenshot shows a web interface for configuring a ping. At the top, the breadcrumb 'IP > General > Ping' is displayed. Below this, there are three input fields: 'Host Name/IP Address' (empty), 'Probe Count (1-16)' (set to 5), and 'Packet Size (IPv4 : 32-1472, IPv6 : 0-512)' (empty). To the right of the packet size field is the unit 'bytes'. Below these fields are two buttons: 'Apply' and 'Revert'. A section titled 'Result' contains a text area with the following output: 'PING to 192.168.0.3, by 5 of 32-byte payload ICMP packets, timeout is 3 seconds', followed by five lines of 'response time: 0 ms' (the first line is '10 ms' in the image), and then 'Ping statistics for 192.168.0.3: 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)', 'Approximate round trip times: Minimum = 0 ms, Maximum = 10 ms, Average = 2 ms'.

USING THE TRACE ROUTE FUNCTION

Use the IP > General > Trace Route page to show the route packets take to the specified destination.

CLI REFERENCES

- ◆ ["traceroute" on page 1372](#)

PARAMETERS

These parameters are displayed:

- ◆ **Destination IP Address** – IPv4/IPv6 address of the host.

COMMAND USAGE

- ◆ Use the trace route function 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 trace route function 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.

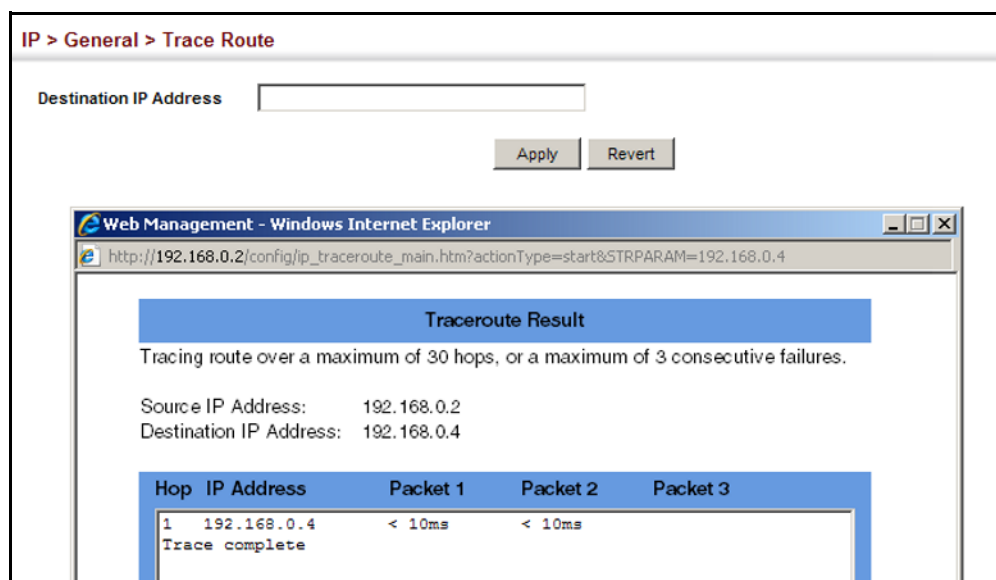
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

WEB INTERFACE

To trace the route to another device on the network:

1. Click IP, General, Trace Route.
2. Specify the target device.
3. Click Apply.

Figure 398: Tracing the Route to a Network Device



ADDRESS RESOLUTION PROTOCOL

If IP routing is enabled (page 671), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC

address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

Table 42: Address Resolution Protocol

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

Also, if the switch receives a request for its own IP address, it will send back a response, and also cache the MAC of the source device's IP address.

**BASIC ARP
CONFIGURATION**

Use the IP > ARP (Configure General) page to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

CLI REFERENCES

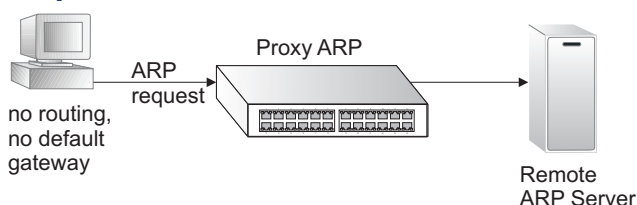
- ◆ ["arp timeout" on page 1376](#)
- ◆ ["ip proxy-arp" on page 1376](#)

COMMAND USAGE

Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.

Figure 399: Proxy ARP



PARAMETERS

These parameters are displayed:

- ◆ **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)

The ARP aging timeout can be set for any configured VLAN.

The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

- ◆ **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces, allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled)

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.

WEB INTERFACE

To configure the timeout for the ARP cache or to enable Proxy ARP for a VLAN (i.e., IP subnetwork):

1. Click IP, ARP.
2. Select Configure General from the Step List.
3. Set the timeout to a suitable value for the ARP cache, or enable Proxy ARP for subnetworks that do not have routing or a default gateway.
4. Click Apply.

Figure 400: Configuring General Settings for ARP

The screenshot shows a web-based configuration interface for ARP settings. At the top, it says "IP > ARP". Below that is a "Step:" dropdown menu set to "1. Configure General". The main configuration area includes a "Timeout (300-86400)" field with a value of "1200" and a "sec" unit. Below this is a "Proxy ARP" section with a "VLAN" dropdown set to "1" and a "Status" checkbox labeled "Enabled". At the bottom right are "Apply" and "Revert" buttons.

CONFIGURING STATIC ARP ADDRESSES

For devices that do not respond to ARP requests or do not respond in a timely manner, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, use the IP > ARP (Configure Static Address – Add) page to manually map an IP address to the corresponding physical address in the ARP cache.

CLI REFERENCES

- ◆ ["arp" on page 1375](#)

COMMAND USAGE

- ◆ The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (that is, Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- ◆ You can define up to 128 static entries in the ARP cache.
- ◆ 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 or deleted when power is reset. You can only remove a static entry via the configuration interface.
- ◆ Static entries are only displayed on the Show page for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of a configure VLAN, and that VLAN is linked up.

PARAMETERS

These parameters are displayed:

- ◆ **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- ◆ **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx)

WEB INTERFACE

To map an IP address to the corresponding physical address in the ARP cache using the web interface:

1. Click IP, ARP.
2. Select Configure Static Address from the Step List.
3. Select Add from the Action List.
4. Enter the IP address and the corresponding MAC address.
5. Click Apply.

Figure 401: Configuring Static ARP Entries

The screenshot shows the 'IP > ARP' web interface. At the top, there is a breadcrumb 'IP > ARP'. Below it, there are two dropdown menus: 'Step: 2. Configure Static Address' and 'Action: Add'. Underneath, there are two input fields: 'IP Address' with the value '10.2.78.105' and 'MAC Address' with the value '00-e0-0c-00-00-fd'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

To display static entries in the ARP cache:

1. Click IP, ARP.
2. Select Configure Static Address from the Step List.
3. Select Show from the Action List.

Figure 402: Displaying Static ARP Entries

The screenshot shows the 'IP > ARP' web interface. At the top, there is a breadcrumb 'IP > ARP'. Below it, there are two dropdown menus: 'Step: 2. Configure Static Address' and 'Action: Show'. Underneath, there is a table titled 'Static Address List' with the following columns: 'IP Address', 'MAC Address', and 'Interface'. The table contains two entries. At the bottom right, there are two buttons: 'Delete' and 'Revert'.

	IP Address	MAC Address	Interface
<input type="checkbox"/>	10.2.78.105	00-E0-0C-00-00-FD	VLAN 1
<input type="checkbox"/>	10.2.78.254	00-12-D9-75-DC-5B	VLAN 1

DISPLAYING DYNAMIC OR LOCAL ARP ENTRIES

Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

CLI REFERENCES

- ◆ "show arp" on page 1377

WEB INTERFACE

To display all dynamic entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Dynamic Address.

Figure 403: Displaying Dynamic ARP Entries

The screenshot shows the 'IP > ARP' web interface. The 'Step' dropdown is set to '3. Show Information'. Under the 'Dynamic Address' radio button, there is a table titled 'Dynamic Address List' with a 'Total: 1' entry. The table has three columns: 'IP Address', 'MAC Address', and 'Interface'. The data row shows IP Address '192.168.2.61', MAC Address '00-60-6E-00-5F-A1', and Interface 'VLAN 1'. There is a 'Clear' button at the bottom right.

IP Address	MAC Address	Interface
192.168.2.61	00-60-6E-00-5F-A1	VLAN 1

To display all local entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Other Address.

Figure 404: Displaying Local ARP Entries

The screenshot shows the 'IP > ARP' web interface. The 'Step' dropdown is set to '3. Show Information'. Under the 'Other Address' radio button, there is a table titled 'Other Address List' with 'Max: 512' and 'Total: 2' entries. The table has three columns: 'IP Address', 'MAC Address', and 'Interface'. The data rows show IP Address '192.168.0.2' and '192.168.2.2', both with MAC Address '00-00-E8-93-82-A0', and Interfaces 'VLAN 2' and 'VLAN 1' respectively.

IP Address	MAC Address	Interface
192.168.0.2	00-00-E8-93-82-A0	VLAN 2
192.168.2.2	00-00-E8-93-82-A0	VLAN 1

DISPLAYING ARP STATISTICS

Use the IP > ARP (Show Information) page to display statistics for ARP messages crossing all interfaces on this router.

CLI REFERENCES

- ◆ "show ip traffic" on page 1411

PARAMETERS

These parameters are displayed:

Table 43: ARP Statistics

Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

WEB INTERFACE

To display ARP statistics:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Statistics.

Figure 405: Displaying ARP Statistics

The screenshot shows the 'IP > ARP' web interface. At the top, there is a breadcrumb 'IP > ARP'. Below it, a 'Step:' dropdown menu is set to '3. Show Information'. Underneath, there are three radio buttons: 'Dynamic Address', 'Other Address', and 'Statistics'. The 'Statistics' radio button is selected. Below the radio buttons, the title 'ARP Statistics' is displayed. The statistics are shown in two columns: 'Received Request' (31), 'Received Reply' (5), 'Sent Request' (5), and 'Sent Reply' (16). At the bottom right, there is a 'Refresh' button.

CONFIGURING STATIC ROUTES

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP). However, you can also manually enter static routes in the routing table using the IP > Routing > Static Routes (Add) page. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

CLI REFERENCES

- ◆ ["ip route" on page 1408](#)

COMMAND USAGE

- ◆ Up to 512 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.
- ◆ If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- ◆ Static routes are included in RIP updates periodically sent by the router if this feature is enabled by RIP (see page 681).

PARAMETERS

These parameters are displayed:

- ◆ **Destination IP Address** – IP address of the destination network, subnetwork, or host.
- ◆ **Netmask / Prefix Length** – 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 router hop used for this route.
- ◆ **Distance** – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 120 for RIP. (Range: 1-255, Default: 1)

WEB INTERFACE

To configure static routes:

1. Click IP, Routing, Static Routes.
2. Select Add from the Action List.
3. Enter the destination address, subnet mask, and next hop router.
4. Click Apply.

Figure 406: Configuring Static Routes

IP > Routing > Static Routes

Action:

Destination IP Address	<input type="text" value="10.2.48.0"/>
Net Mask / Prefix Length	<input type="text" value="255.255.255.0"/>
Next Hop	<input type="text" value="10.2.48.1"/>
Distance (1-255)	<input type="text" value="5"/> (Optional)

To display static routes:

1. Click IP, Routing, Static Routes.
2. Select Show from the Action List.

Figure 407: Displaying Static Routes

IP > Routing > Static Routes

Action: Show

Static Table List Total: 3

<input type="checkbox"/>	Destination IP Address	Net Mask / Prefix Length	Next Hop	Distance
<input type="checkbox"/>	10.2.48.2	255.255.255.0	10.2.48.1	5
<input type="checkbox"/>	10.5.36.123	255.255.0.0	10.5.36.1	2
<input type="checkbox"/>	5566::	60	7788::12	1

Delete Revert

DISPLAYING THE ROUTING TABLE

Use the IP > Routing > Routing Table (Show Information) page to display all routes that can be accessed via local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic (except when the distance parameter of a dynamic route is set to a value that makes its priority exceed that of a static route). Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

CLI REFERENCES

- ◆ ["show ip route" on page 1409](#)

COMMAND USAGE

- ◆ The Forwarding Information Base (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 – RIB), which holds all routing information received from routing peers. The FIB 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 FIB entry are a network prefix, a router (i.e., VLAN) interface, and next hop information.

- ◆ The Routing Table (and [show ip route](#) 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 dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the [show ip route database](#) command.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier (i.e., configure as a valid IP subnet).
- ◆ **Destination IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- ◆ **Net Mask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ◆ **Next Hop** – The IP address of the next hop (or gateway) in this route.
- ◆ **Metric** – Cost for this interface.
- ◆ **Protocol** – The protocol which generated this route information. (Options: Local, Static, RIP, OSPF, Others)

WEB INTERFACE

To display the routing table:

1. Click IP, Routing, Routing Table.
2. Select Show Information from the Action List.

Figure 408: Displaying the Routing Table

IP > Routing > Routing Table					
Action: Show Information ▼					
Routing Table List Total: 5					
VLAN	Destination IP Address	Net Mask / Prefix Length	Next Hop	Metric	Protocol
0	127.0.0.0	255.0.0.0	--	0	Local
2	192.168.0.0	255.255.255.0	--	0	Local
1	192.168.2.0	255.255.255.0	--	0	Local
2	192.168.3.0	255.255.255.0	192.168.0.1	0	Static
0	::1	128	--	0	Local

This chapter describes how to configure the following unicast routing protocols:

RIP – Configures Routing Information Protocol.

OVERVIEW

This switch can route unicast traffic to different subnetworks using the Routing Information Protocol (RIP). It supports RIP and RIP-2 dynamic routing. These protocols exchange routing information, calculate routing tables, and can respond to changes in the status or loading of the network.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

Non-IP Protocol Routing

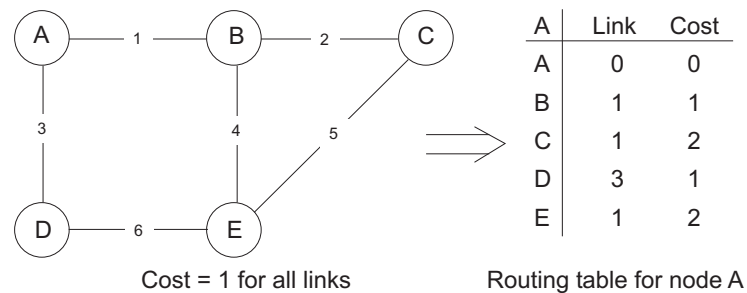
The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

CONFIGURING THE ROUTING INFORMATION PROTOCOL

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

Figure 409: Configuring RIP



COMMAND USAGE

- ◆ Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:
 - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
 - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
 - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.
- ◆ RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).
- ◆ There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

CONFIGURING GENERAL PROTOCOL SETTINGS

Use the Routing Protocol > RIP > General (Configure) page to configure general settings and the basic timers.

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (see ["Configuring Network Interfaces for RIP" on page 685](#)).

CLI REFERENCES

- ◆ ["Routing Information Protocol \(RIP\)" on page 1412](#)

COMMAND USAGE

- ◆ RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces ([page 685](#)).

PARAMETERS

These parameters are displayed:

Global Settings

- ◆ **RIP Routing Process** – Enables RIP routing globally. RIP must also be enabled on each network interface which will participate in the routing process as described under ["Specifying Network Interfaces" on page 677](#). (Default: Disabled)
- ◆ **Global RIP Version** – Specifies a RIP version used globally by the router. (Version 1, Version 2, By Interface; Default: By Interface)

When a Global RIP Version is specified, any VLAN interface not previously set to a specific Receive or Send Version ([page 685](#)) is set to the following values:

- RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
- RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.

RIP send/receive versions set on the RIP Interface settings screen ([page 685](#)) always take precedence over the settings for the Global RIP Version. However, when the Global RIP Version is set to "By Interface," any VLAN interface not previously set to a specific receive or send version is set to the following default values:

- Receive: Accepts RIPv1 or RIPv2 packets.
- Send: Route information is broadcast to other routers with RIPv2.

- ◆ **RIP Default Metric** – Sets the default metric assigned to external routes imported from other protocols. (Range: 1-15; Default: 1)

The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

The default metric does not override the metric value set in the Redistribute screen (see ["Configuring Route Redistribution" on page 681](#)). When a metric value has not been configured in the Redistribute screen, the default metric sets the metric value to be used for all imported external routes.

- ◆ **RIP Max Prefix** – Sets the maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168; Default: 7168)

- ◆ **Default Information Originate** – Generates a default external route into the local RIP autonomous system. (Default: Disabled)

A default route is set for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

- ◆ **Default Distance** – Defines an administrative distance for external routes learned from other routing protocols. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255; Default: 120)

Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

Use the Routing Protocol > RIP > Distance page (see [page 683](#)) to configure the distance to a specific network address, or to configure an access list that filters networks according to the IP address of the router supplying the routing information.

- ◆ **Number of Route Changes** – The number of route changes made to the IP route database by RIP.

- ◆ **Number of Queries** – The number of responses sent to RIP queries from other systems.

Basic Timer Settings



NOTE: The timers must be set to the same values for all routers in the network.

- ◆ **Update** – Sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
(Range: 5-2147483647 seconds; Default: 30 seconds)

Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.
- ◆ **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
(Range: 90-360 seconds; Default: 180 seconds)
- ◆ **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging.
(Range: 60-240 seconds; Default: 120 seconds)

WEB INTERFACE

To configure general settings for RIP:

1. Click Routing Protocol, RIP, General.
2. Select Configure Global from the Action list.
3. Enable RIP, set the RIP version used on unset interfaces to RIPv1 or RIPv2, set the default metric assigned to external routes, set the maximum number of routes allowed by the system, and set the basic timers.
4. Click Apply.

Figure 410: Configuring General Settings for RIP

The screenshot shows the 'Routing Protocol > RIP > General' configuration page. At the top, there is a breadcrumb trail and an 'Action:' dropdown menu set to 'Configure'. Below this, the 'Global' section contains the following settings:

- RIP Routing Process: ☒ Enabled
- Global RIP Version: By interface (dropdown)
- RIP Default Metric (1-15): 1
- RIP Max Prefix (1-7168): 7168
- Default Information Originate: ☐ Enabled
- Default Distance (1-255): 120
- Number of Route Changes: 0
- Number of Queries: 0

The 'Basic Timer' section contains the following settings:

- Update (5-2147483647): 30 sec
- Timeout (90-360): 180 sec
- Garbage Collection (60-240): 120 sec

At the bottom right, there are 'Apply' and 'Revert' buttons.

CLEARING ENTRIES FROM THE ROUTING TABLE

Use the Routing Protocol > RIP > General (Clear Route) page to clear entries from the routing table based on route type or a specific network address.

CLI REFERENCES

- ◆ "clear ip rip route" on page 1427

COMMAND USAGE

- ◆ Clearing "All" types deletes all routes in the RIP table. To avoid deleting the entire RIP network, redistribute connected routes using the Routing Protocol > RIP > Redistribute screen ([page 681](#)) to make the RIP network a connected route. To delete the RIP routes learned from neighbors, but keep the RIP network intact, clear "RIP" types from the routing table.

PARAMETERS

These parameters are displayed:

- ◆ **Clear Route By Type** – Clears entries from the RIP routing table based on the following types:
 - **All** – Deletes all entries from the routing table.
 - **Connected** – Deletes all currently connected entries.
 - **RIP** – Deletes all entries learned through the RIP.
 - **Static** – Deletes all static entries.

- ◆ **Clear Route By Network** – Clears a specific route based on its IP address and prefix length.
 - **Network IP Address** – Deletes all related entries for the specified network address.
 - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the network portion of the address.

WEB INTERFACE

To clear entries from the routing table RIP:

1. Click Routing Protocol, RIP, General.
2. Select Clear Route from the Action list.
3. When clearing routes by type, select the required type from the drop-down list. When clearing routes by network, enter a valid network address and prefix length.
4. Click Apply.

Figure 411: Clearing Entries from the Routing Table

Routing Protocol > RIP > General

Action: Clear Route ▼

Clear Route by: ☐ Type ☒ Network

Network IP Address: 192.168.1.0

Prefix Length (1-32): 24

Apply Revert

SPECIFYING NETWORK INTERFACES Use the Routing Protocol > RIP > Network (Add) page to specify the network interfaces that will be included in the RIP routing process.

CLI REFERENCES

- ◆ ["network" on page 1417](#)

COMMAND USAGE

- ◆ RIP only sends and receives updates on specified interfaces. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.
- ◆ No networks are specified by default.

PARAMETERS

These parameters are displayed:

- ◆ **By Address** – Adds a network to the RIP routing process.
 - **Subnet Address** – IP address of a network directly connected to this router. (Default: No networks are specified)
 - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the network portion of the address. This mask identifies the network address bits used for the associated routing entries.
- ◆ **By VLAN** – Adds a Layer 3 VLAN to the RIP routing process. The VLAN must be configured with an IP address. (Range: 1-4093)

WEB INTERFACE

To add a network interface to RIP:

1. Click Routing Protocol, RIP, Network.
2. Select Add from the Action list.
3. Add an interface that will participate in RIP.
4. Click Apply.

Figure 412: Adding Network Interfaces to RIP

Routing Protocol > RIP > Network

Action: Add ▼

By ☒ IP Address ☐ VLAN

Subnet Address 10.1.0.0

Prefix Length (1-32) 16

Apply Revert

To show the network interfaces using RIP:

1. Click Routing Protocol, RIP, Network.
2. Select Show from the Action list.
3. Click IP Address or VLAN.

Figure 413: Showing Network Interfaces Using RIP

Routing Protocol > RIP > Network

Action: Show

By: ☒ IP Address ☐ VLAN

RIP Network Address List Total: 1

	Subnet Address	Prefix Length
<input type="checkbox"/>	10.1.0.0	16

Delete Revert

SPECIFYING PASSIVE INTERFACES

Use the Routing Protocol > RIP > Passive Interface (Add) page to stop RIP from sending routing updates on the specified interface.

CLI REFERENCES

- ◆ ["passive-interface" on page 1418](#)

COMMAND USAGE

- ◆ Network interfaces can be configured to stop RIP broadcast and multicast messages from being sent. If the sending of routing updates is blocked on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on the specified interface will continue to be received and processed.
- ◆ This feature can be used in conjunction with the static neighbor feature (described in the next section) to control the routing updates sent to specific neighbors.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – VLAN interface on which to stop sending RIP updates. (Range: 1-4093)

WEB INTERFACE

To specify a passive RIP interface:

1. Click Routing Protocol, RIP, Passive Interface.
2. Select Add from the Action list.
3. Add the interface on which to stop sending RIP updates.
4. Click Apply.

Figure 414: Specifying a Passive RIP Interface

Routing Protocol > RIP > Passive Interface

Action: Add

VLAN ID (1-4093) 1

Apply Revert

To show the passive RIP interfaces:

1. Click Routing Protocol, RIP, Passive Interface.
2. Select Show from the Action list.

Figure 415: Showing Passive RIP Interfaces

Routing Protocol > RIP > Passive Interface

Action: Show

VLAN ID List Total: 1

	VLAN ID
<input type="checkbox"/>	1

Delete Revert

SPECIFYING STATIC NEIGHBORS

Use the Routing Protocol > RIP > Passive Interface (Add) page to configure this router to directly exchange routing information with a static neighbor (specifically for point-to-point links), rather than relying on broadcast or multicast messages generated by the RIP protocol. This feature can be used in conjunction with the passive interface feature (described in the preceding section) to control the routing updates sent to specific neighbors.

CLI REFERENCES

- ◆ ["neighbor" on page 1416](#)

PARAMETERS

These parameters are displayed:

- ◆ **IP Address** – IP address of a static neighboring router with which to exchange routing information.

WEB INTERFACE

To specify a static RIP neighbor:

1. Click Routing Protocol, RIP, Neighbor Address.
2. Select Add from the Action list.

3. Add the address of any static neighbors which may not readily to discovered through RIP.
4. Click Apply.

Figure 416: Specifying a Static RIP Neighbor

Routing Protocol > RIP > Neighbor Address

Action: Add

IP Address 10.2.0.254

Apply Revert

To show static RIP neighbors:

1. Click Routing Protocol, RIP, Neighbor Address.
2. Select Show from the Action list.

Figure 417: Showing Static RIP Neighbors

Routing Protocol > RIP > Neighbor Address

Action: Show

Neighbor Address List Total: 1

	IP Address
<input type="checkbox"/>	10.2.0.254

Delete Revert

CONFIGURING ROUTE REDISTRIBUTION

Use the Routing Protocol > RIP > Redistribute (Add) page to import external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into this autonomous system.

CLI REFERENCES

- ◆ ["redistribute" on page 1418](#)

PARAMETERS

These parameters are displayed:

- ◆ **Protocol** – The type of routes that can be imported include:
 - **Connected** – Imports routes that are established automatically just by enabling IP on an interface.
 - **Static** – Static routes will be imported into this routing domain.
 - **OSPF** – External routes will be imported from the Open Shortest Path First protocol into this routing domain.

- ◆ **Metric** – Metric assigned to all external routes for the specified protocol. (Range: 0-16; Default: the default metric as described under ["Configuring General Protocol Settings" on page 673.](#))

A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

When a metric value has not been configured on this page, the default-metric determines the metric value to be used for all imported external routes.

It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow an imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

WEB INTERFACE

To import external routing information from other routing domains:

1. Click Routing Protocol, RIP, Redistribute.
2. Select Add from the Action list.
3. Specify the protocol types (directly connected, OSPF or static) from which to import external routes, and the metric to assign to these routes.
4. Click Apply.

Figure 418: Redistributing External Routes into RIP

Routing Protocol > RIP > Redistribute

Action:

Protocol:

Metric (1-16): (Optional)

To show external routes imported into RIP:

1. Click Routing Protocol, RIP, Redistribute.
2. Select Show from the Action list.

Figure 419: Showing External Routes Redistributed into RIP

Routing Protocol > RIP > Redistribute

Action: Show

Redistribute List Total: 1

<input type="checkbox"/>	Protocol	Metric
<input type="checkbox"/>	OSPF	3

Delete Revert

SPECIFYING AN ADMINISTRATIVE DISTANCE

Use the Routing Protocol > RIP > Distance (Add) page to define an administrative distance for external routes learned from other routing protocols.

CLI REFERENCES

- ◆ ["distance" on page 1415](#)

COMMAND USAGE

- ◆ Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.
- ◆ An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.
- ◆ The administrative distance is applied to all routes learned for the specified network.

PARAMETERS

These parameters are displayed:

- ◆ **Distance** – Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255)
- ◆ **IP Address** – IP address of a route entry.
- ◆ **Subnet Mask** – This mask identifies the host address bits used for associated routing entries.
- ◆ **ACL Name** – Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

WEB INTERFACE

To define an administrative distance for external routes learned from other routing protocols:

1. Click Routing Protocol, RIP, Distance.
2. Select Add from the Action list.
3. Enter the distance, the external route, and optionally enter the name of an ACL to filter networks according to the IP address of the router supplying the routing information.
4. Click Apply.

Figure 420: Setting the Distance Assigned to External Routes

Routing Protocol > RIP > Distance

Action: Add

Distance (1-255): 120

IP Address: 192.168.3.0

Subnet Mask: 255.255.255.0

ACL Name: ☐

Apply Revert

To show the distance assigned to external routes learned from other routing protocols:

1. Click Routing Protocol, RIP, Distance.
2. Select Show from the Action list.

Figure 421: Showing the Distance Assigned to External Routes

Routing Protocol > RIP > Distance

Action: Show

RIP Distance List Total: 1

	Distance	IP Address	Subnet Mask	ACL Name
<input type="checkbox"/>	120	192.168.3.0	255.255.255.0	

Delete Revert

CONFIGURING NETWORK INTERFACES FOR RIP Use the Routing Protocol > RIP > Distance (Add) page to configure the send/receive version, authentication settings, and the loopback prevention method for each interface that participates in the RIP routing process.

CLI REFERENCES

- ◆ "ip rip receive version" on page 1423
- ◆ "ip rip send version" on page 1425
- ◆ "ip rip authentication mode" on page 1422
- ◆ "ip rip authentication string" on page 1423
- ◆ "ip rip split-horizon" on page 1426

COMMAND USAGE

Specifying Receive and Send Protocol Types

- ◆ Specify the protocol message type accepted (that is, RIP version) and the message type sent (that is, RIP version or compatibility mode) for each RIP interface.
- ◆ Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified in the RIP General Settings screen (see ["Configuring General Protocol Settings" on page 673](#)).
- ◆ The Send Version can be specified based on these options:
 - Use "RIPv1" or "RIPv2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use "RIPv1 Compatible" to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information. (This is the default setting.)
 - Use "Do Not Send" to passively monitor route information advertised by other routers attached to the network.
- ◆ The Receive Version can be specified based on these options:
 - Use "RIPv1" or "RIPv2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use "RIPv1 and RIPv2" if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1. (This is the default setting.)
 - Use "Do Not Receive" if dynamic entries are not required to be added to the routing table for an interface. (For example, when only static routes are to be allowed for a specific interface.)

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or

unwanted protocol messages can be easily propagated throughout the network if no authentication is required.

RIPv2 supports authentication using a simple password or MD5 key encryption. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP supports several methods which can provide faster convergence when the network topology changes and prevent most loops from occurring.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN ID** – Layer 3 VLAN interface. This interface must be configured with an IP address and have an active link. (Range: 1-4093)
- ◆ **Send Version** – The RIP version to send on an interface.
 - **RIPv1**: Sends only RIPv1 packets.
 - **RIPv2**: Sends only RIPv2 packets.
 - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2.
 - **Do Not Send**: Does not transmit RIP updates. Passively monitors route information advertised by other routers attached to the network.

The default depends on the setting for the Global RIP Version. (See ["Configuring General Protocol Settings" on page 673.](#))

- ◆ **Receive Version** – The RIP version to receive on an interface.
 - **RIPv1**: Accepts only RIPv1 packets.
 - **RIPv2**: Accepts only RIPv2 packets.
 - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets.

- **Do Not Receive:** Does not accept incoming RIP packets. This option does not add any dynamic entries to the routing table for an interface.

The default depends on the setting for the Global RIP Version. (See ["Configuring General Protocol Settings" on page 673.](#))

- ◆ **Authentication Type** – Specifies the type of authentication required for exchanging RIPv2 protocol messages. (Default: No Authentication)

- **No Authentication:** No authentication is required.
- **Simple Password:** Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
- **MD5:** Message Digest 5 (MD5) authentication.

MD5 is a one-way hash algorithm that takes the authentication key and produces a 128 bit message digest or "fingerprint." This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

- ◆ **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)
- ◆ **Instability Prevention** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router.
 - **Split Horizon** – This method never propagate routes back to an interface from which they have been acquired.
 - **Poison Reverse** – This method propagates routes back to an interface from which they have been acquired, but sets the distance-vector metrics to infinity. This provides faster convergence. (This is the default setting.)
 - **None** – No loopback prevention method is employed. If a loop occurs without using any prevention method, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

WEB INTERFACE

To network interface settings for RIP:

1. Click Routing Protocol, RIP, Interface.
2. Select Add from the Action list.
3. Select a Layer 3 VLAN interface to participate in RIP. Select the RIP protocol message types that will be received and sent. Select the RIP authentication method and password. And then set the loopback prevention method.
4. Click Apply.

Figure 422: Configuring a Network Interface for RIP

Routing Protocol > RIP > Interface

Action: Add

VLAN ID (1-4093): 1

Send Version: RIPv1 Compatible

Receive Version: RIPv1 and RIPv2

Authentication Type: Simple Password

Authentication Key: mighty

Instability Prevention: Poison Reverse

Apply Revert

To show the network interface settings configured for RIP:

1. Click Routing Protocol, RIP, Interface.
2. Select Show from the Action list.

Figure 423: Showing RIP Network Interface Settings

Routing Protocol > RIP > Interface

Action: Show

Interface Settings List Total: 2

<input type="checkbox"/>	VLAN ID	Send Version	Receive Version	Authentication Type	Authentication Key	Instability Prevention
<input type="checkbox"/>	1	RIPv1 Compatible	RIPv1 and RIPv2	Simple Password	mighty	Poison Reverse
<input type="checkbox"/>	2	RIPv1 Compatible	RIPv1 and RIPv2	No Authentication		Poison Reverse

Delete Revert

DISPLAYING RIP INTERFACE SETTINGS Use the Routing Protocol > RIP > Statistics (Show Interface Information) page to display information about RIP interface configuration settings.

CLI REFERENCES

- ◆ "show ip rip" on page 1428

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Source IP address of RIP router interface.
- ◆ **Auth Type** – The type of authentication used for exchanging RIPv2 protocol messages.
- ◆ **Send Version** – The RIP version to sent on this interface.
- ◆ **Receive Version** – The RIP version accepted on this interface.
- ◆ **Rcv Bad Packets** – Number of bad RIP packets received.
- ◆ **Rcv Bad Routes** – Number of bad routes received.
- ◆ **Send Updates** – Number of route changes.

WEB INTERFACE

To display RIP interface configuration settings:

1. Click Routing Protocol, RIP, Statistics.
2. Select Show Interface Information from the Action list.

Figure 424: Showing RIP Interface Settings

Routing Protocol > RIP > Statistics						
Action: Show Interface Information						
Interface Information Total: 3						
Interface	Auth Type	Send Version	Receive Version	Rcv Bad Packets	Rcv Bad Routes	Send Updates
1.2.3.4	No Authentication	Do Not Send	RIPv1 and RIPv2	10	2	124
10.1.0.1	Simple Password	RIPv1	Do Not Receive	3	4	23
140.113.1.3	MD5	RIPv1 Compatible	RIPv2	5	5	65

DISPLAYING PEER ROUTER INFORMATION Use the Routing Protocol > RIP > Statistics (Show Peer Information) page to display information on neighboring RIP routers.

CLI REFERENCES

- ◆ "show ip protocols rip" on page 1428

PARAMETERS

These parameters are displayed:

- ◆ **Peer Address** – IP address of a neighboring RIP router.

- ◆ **Update Time** – Last time a route update was received from this peer.
- ◆ **Version** – Shows whether RIPv1 or RIPv2 packets were received from this peer.
- ◆ **Rcv Bad Packets** – Number of bad RIP packets received from this peer.
- ◆ **Rcv Bad Routes** – Number of bad routes received from this peer.

WEB INTERFACE

To display information on neighboring RIP routers:

1. Click Routing Protocol, RIP, Statistics.
2. Select Show Peer Information from the Action list.

Figure 425: Showing RIP Peer Information

Routing Protocol > RIP > Statistics				
Action: Show Peer Information				
Peer Information Total: 2				
Peer Address	Update Time	Version	Rcv Bad Packets	Rcv Bad Routes
10.2.3.0	10	RIPv1	2	123
10.1.0.0	113	RIPv2	4	23

RESETTING RIP STATISTICS

Use the Routing Protocol > RIP > Statistics (Reset Statistics) page to reset all statistics for RIP protocol messages.

CLI REFERENCES

- ◆ no comparable command

WEB INTERFACE

To reset RIP statistics:

1. Click Routing Protocol, RIP, Statistics.
2. Select Reset Statistics from the Action list.
3. Click Reset.

Figure 426: Resetting RIP Statistics

Routing Protocol > RIP > Statistics	
Action: Reset Statistics	
<div>Reset Click the button to reset RIP statistics.</div>	

SECTION III

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 693](#)
- ◆ ["General Commands" on page 707](#)
- ◆ ["System Management Commands" on page 715](#)
- ◆ ["SNMP Commands" on page 785](#)
- ◆ ["Remote Monitoring Commands" on page 807](#)
- ◆ ["Flow Sampling Commands" on page 815](#)
- ◆ ["Authentication Commands" on page 823](#)
- ◆ ["General Security Measures" on page 887](#)
- ◆ ["Access Control Lists" on page 949](#)
- ◆ ["Interface Commands" on page 973](#)
- ◆ ["Link Aggregation Commands" on page 993](#)
- ◆ ["Power over Ethernet Commands" on page 1007](#)
- ◆ ["Port Mirroring Commands" on page 1013](#)
- ◆ ["Rate Limit Commands" on page 1023](#)
- ◆ ["Automatic Traffic Control Commands" on page 1025](#)
- ◆ ["Loopback Detection Commands" on page 1041](#)
- ◆ ["UniDirectional Link Detection Commands" on page 1047](#)
- ◆ ["Address Table Commands" on page 1053](#)

- ◆ "Spanning Tree Commands" on page 1059
- ◆ "ERPS Commands" on page 1087
- ◆ "VLAN Commands" on page 1119
- ◆ "Class of Service Commands" on page 1167
- ◆ "Quality of Service Commands" on page 1181
- ◆ "Multicast Filtering Commands" on page 1201
- ◆ "LLDP Commands" on page 1269
- ◆ "CFM Commands" on page 1295
- ◆ "OAM Commands" on page 1337
- ◆ "Domain Name Service Commands" on page 1347
- ◆ "DHCP Commands" on page 1357
- ◆ "IP Interface Commands" on page 1367
- ◆ "IP Routing Commands" on page 1407

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

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 ECS4510-28T 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 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 ECS4510-28T 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:

```
Console>enable  
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 an accounting list with this name
arp               Information of ARP cache
authorization     Enables EXEC accounting
auto-traffic-control Auto traffic control information
banner            Banner info
bridge-ext        Bridge extension information
cable-diagnostics Shows the information of cable diagnostics
calendar          Date and time information
class-map         Displays class maps
cluster           Display cluster
debug             State of each debugging option
dns               DNS information
dos-protection    Shows the system dos-protection summary information
dot1q-tunnel      dot1q-tunnel
dot1x             802.1X content
efm               Ethernet First Mile feature
erps              Displays ERPS configuration
ethernet          Specifies the ethernet
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
line              TTY line information
lldp              LLDP
log               Log records
logging           Logging setting
loop              Shows the information of loopback
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             Shows power
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 Protocol
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
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
udld	Displays UDLD information
upgrade	Shows upgrade information
users	Information about users logged in
version	System hardware and software versions
vlan	Shows virtual LAN settings
vlan-translation	VLAN translation information
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
protocol-vlan	Protocol-VLAN information
status	Shows interface status
switchport	Shows interface switchport information
transceiver	Interface of transceiver 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          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 44: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List CFM Class Map ERPS IGMP Profile Interface Line Multiple Spanning Tree Policy Map Router 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 ECS4510-28T is opened.
To end the CLI session, enter [Exit].

Console#

```

```

Username: guest
Password: [guest login password]

CLI session with the ECS4510-28T 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.
- ◆ CFM Configuration - 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.
- ◆ Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- ◆ ERPS Configuration - These commands configure Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks.
- ◆ 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.
- ◆ Router Configuration - These commands configure global settings for unicast routing protocols.
- ◆ 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 45: Configuration Command Modes

Mode	Command	Prompt	Page
Access Control List	access-list arp	Console(config-arp-acl)	967
	access-list ip standard	Console(config-std-acl)	950
	access-list ip extended	Console(config-ext-acl)	950
	access-list ipv6 standard	Console(config-std-ipv6-acl)	956
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	956
	access-list mac	Console(config-mac-acl)	962
CFM	ethernet cfm domain	Console(config-ether-cfm)	1301
Class Map	class-map	Console(config-cmap)	1182
ERPS	erps domain	Console(config-erps)	1089
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)	974
Line	line {console vty}	Console(config-line)	747
MSTP	spanning-tree mst-configuration	Console(config-mstp)	1066
Policy Map	policy-map	Console(config-pmap)	1186
Router	router rip	Console(config-router)	1413
Time Range	time-range	Console(config-time-range)	776
VLAN	vlan database	Console(config-vlan)	1125

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 46: Keystroke Commands

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

SHOWING STATUS INFORMATION

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

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

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

```

VLAN M'cast Router Ports Type
-----
1      Eth 1/11          Static
Console#

```

CLI COMMAND GROUPS

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

Table 47: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	707
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	715
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	785
Remote Monitoring	Supports statistics, history, alarm and event groups	807
Flow sampling	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	815
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	823
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	887
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)	949
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	973
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	993
Power over Ethernet	Configures power output for connected devices	1007
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	1013
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	1023
Automatic Traffic Control	Configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port	1025

Table 47: Command Group Index (Continued)

Command Group	Description	Page
Loopback Detection	Detects general loopback conditions caused by hardware problems or faulty protocol settings	1041
UniDirectional Link Detection	Detect and disables unidirectional links	1047
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	1053
Spanning Tree	Configures Spanning Tree settings for the switch	1059
ERPS	Configures Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks	1087
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	1119
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	1167
Quality of Service	Configures Differentiated Services	1181
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration	1201
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	1269
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	1295
OAM	Configures Operations, Administration and Maintenance remote management tools required to monitor and maintain the links to subscriber CPEs	1337
Domain Name Service	Configures DNS services.	1347
Dynamic Host Configuration Protocol	Configures DHCP client and relay functions	1357
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters	1367
IP Routing	Configures static and dynamic unicast routing	1407

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)
RC (Router Configuration)
VC (VLAN Database Configuration)

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

Table 48: 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

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**} | **regularity** *hour minute* [**period** {**daily** | **weekly** *day-of-week* | **monthly** *day*}] | **cancel** [**at** | **in** | **regularity**]}

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: 2001-2050)

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 regularity - 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 - 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 736](#)).

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 2007 ---
***

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 698](#).

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 \(712\)](#)[enable password \(824\)](#)

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 698](#).

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#configure
Console(config)#

```

RELATED COMMANDS

[end \(713\)](#)

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 698](#).

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 \(709\)](#)

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 2001.
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:

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 49: System Management Commands

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
Banner Information	Configures administrative contact, device identification and location
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 50: 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

EXAMPLE

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

BANNER INFORMATION

These commands are used to configure and manage administrative information about the switch, its exact data center location, details of the electrical and network circuits that supply the switch, as well as contact information for the network administrator and system manager. This information is only available via the CLI and is automatically displayed before login as soon as a console or telnet connection has been established.

Table 51: Banner Commands

Command	Function	Mode
banner configure	Configures the banner information that is displayed before login	GC
banner configure company	Configures the Company information that is displayed by banner	GC
banner configure dc-power-info	Configures the DC Power information that is displayed by banner	GC
banner configure department	Configures the Department information that is displayed by banner	GC
banner configure equipment-info	Configures the Equipment information that is displayed by banner	GC
banner configure equipment-location	Configures the Equipment Location information that is displayed by banner	GC
banner configure ip-lan	Configures the IP and LAN information that is displayed by banner	GC
banner configure lp-number	Configures the LP Number information that is displayed by banner	GC

Table 51: Banner Commands (Continued)

Command	Function	Mode
<code>banner configure manager-info</code>	Configures the Manager contact information that is displayed by banner	GC
<code>banner configure mux</code>	Configures the MUX information that is displayed by banner	GC
<code>banner configure note</code>	Configures miscellaneous information that is displayed by banner under the Notes heading	GC
<code>show banner</code>	Displays all banner information	NE, PE

banner configure This command is used to interactively specify administrative information for this device.

SYNTAX

`banner configure`

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The administrator can batch-input all details for the switch with one command. When the administrator finishes typing the company name and presses the enter key, the script prompts for the next piece of information, and so on, until all information has been entered. Pressing enter without inputting information at any prompt during the script's operation will leave the field empty. Spaces can be used during script mode because pressing the enter key signifies the end of data input. The delete and left-arrow keys terminate the script. The use of the backspace key during script mode is not supported. If, for example, a mistake is made in the company name, it can be corrected with the **banner configure company** command.

EXAMPLE

```

Console(config)#banner configure

Company: Edge-Core Networks
Responsible department: R&D Dept
Name and telephone to Contact the management people
Manager1 name: Sr. Network Admin
  phone number: 123-555-1212
Manager2 name: Jr. Network Admin
  phone number: 123-555-1213
Manager3 name: Night-shift Net Admin / Janitor
  phone number: 123-555-1214
The physical location of the equipment.
City and street address: 12 Straight St. Motown, Zimbabwe
Information about this equipment:
Manufacturer: Edge-Core Networks
ID: 123_unique_id_number
Floor: 2

```

```
Row: 7
Rack: 29
Shelf in this rack: 8
Information about DC power supply.
Floor: 2
Row: 7
Rack: 25
Electrical circuit: : ec-177743209-xb
Number of LP:12
Position of the equipment in the MUX:1/23
IP LAN:192.168.1.1
Note: This is a random note about this managed switch and can contain
      miscellaneous information.
Console(config)#
```

banner configure company This command is used to configure company information displayed in the banner. Use the **no** form to remove the company name from the banner display.

SYNTAX

banner configure company *name*

no banner configure company

name - The name of the company.
(Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure company** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure company Big-Ben
Console(config)#
```

banner configure dc-power-info This command is use to configure DC power information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure dc-power-info floor *floor-id* **row** *row-id*
rack *rack-id* **electrical-circuit** *ec-id*

no banner configure dc-power-info [**floor** | **row** | **rack** | **electrical-circuit**]

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

ec-id - The electrical circuit ID.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure dc-power-info** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure dc-power-info floor 3 row 15 rack 24
                    electrical-circuit 48v-id_3.15.24.2
Console(config)#
```

banner configure department This command is used to configure the department information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure department *dept-name*

no banner configure department

dept-name - The name of the department.
(Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure department** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure department R&D
Console(config)#
```

banner configure equipment-info This command is used to configure the equipment information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure equipment-info manufacturer-id *mfr-id*
floor *floor-id* **row** *row-id* **rack** *rack-id* **shelf-rack** *sr-id*
manufacturer *mfr-name*

no banner configure equipment-info [**floor** | **manufacturer** |
manufacturer-id | **rack** | **row** | **shelf-rack**]

mfr-id - The name of the device model number.

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

sr-id - The shelf number in the rack.

mfr-name - The name of the device manufacturer.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure equipment-info** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure equipment-info manufacturer-id ECS4510-28T
floor 3 row 10 rack 15 shelf-rack 12 manufacturer Edge-Core
Console(config)#
```

**banner configure
equipment-location**

This command is used to configure the equipment location information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure equipment-location *location*

no banner configure equipment-location

location - The address location of the device.
(Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure equipment-location** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure equipment-location
710_Network_Path,_Indianapolis
Console(config)#
```

**banner configure ip-
lan**

This command is used to configure the device IP address and subnet mask information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure ip-lan *ip-mask*

no banner configure ip-lan

ip-mask - The IP address and subnet mask of the device.
(Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure ip-lan** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure ip-lan 192.168.1.1/255.255.255.0  
Console(config)#
```

banner configure lp-number

This command is used to configure the LP number information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure lp-number *lp-num*

no banner configure lp-number

lp-num - The LP number. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure lp-number** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure lp-number 12  
Console(config)#
```

banner configure manager-info This command is used to configure the manager contact information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

```
banner configure manager-info
  name mgr1-name phone-number mgr1-number
  [name2 mgr2-name phone-number mgr2-number |
  name3 mgr3-name phone-number mgr3-number]

no banner configure manager-info [name1 | name2 | name3]

mgr1-name - The name of the first manager.
mgr1-number - The phone number of the first manager.
mgr2-name - The name of the second manager.
mgr2-number - The phone number of the second manager.
mgr3-name - The name of the third manager.
mgr3-number - The phone number of the third manager.
Maximum length of each parameter: 32 characters
```

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure manager-info** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure manager-info name Albert_Einstein phone-
number 123-555-1212 name2 Lamar phone-number 123-555-1219
Console(config)#
```

banner configure mux This command is used to configure the mux information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

```
banner configure mux muxinfo

no banner configure mux

muxinfo - The circuit and PVC to which the switch is connected.
(Maximum length: 32 characters)
```

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure mux** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure mux telco-8734212kx_PVC-1/23
Console(config)#
```

banner configure note This command is used to configure the note displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure note *note-info*

no banner configure note

note-info - Miscellaneous information that does not fit the other banner categories, or any other information of importance to users of the switch CLI. (Maximum length: 150 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure note** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure note !!!!!ROUTINE_MAINTENANCE_firmware-
upgrade_0100-0500_GMT-0500_20071022!!!!_20min_network_impact_expected
Console(config)#
```


show banner This command displays all banner information.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show banner
Edge-Core
WARNING - MONITORED ACTIONS AND ACCESSES
R&D

Albert_Einstein - 123-555-1212
Lamar - 123-555-1219

Station's information:
710_Network_Path,_Indianapolis

ECS4510-28T
Floor / Row / Rack / Sub-Rack
3/ 10 / 15 / 12
DC power supply:
Power Source A: Floor / Row / Rack / Electrical circuit
3/ 15 / 24 / 48v-id_3.15.24.2
Number of LP: 12
Position MUX: telco-8734212kx_PVC-1/23
IP LAN: 192.168.1.1/255.255.255.0
Note: !!!!!ROUTINE_MAINTENANCE_firmware-upgrade_0100-0500_GMT-
0500_20071022!!!!!!_20min_network_
Console#
```

SYSTEM STATUS

This section describes commands used to display system information.

Table 52: System Status Commands

Command	Function	Mode
show access-list tcam-utilization	Shows utilization parameters for TCAM	PE
show memory	Shows memory utilization parameters	NE, PE
show process cpu	Shows CPU utilization parameters	NE, PE
show running-config	Displays the configuration data currently in use	PE
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show system	Displays system information	NE, PE
show tech-support	Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems	PE
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE
show version	Displays version information for the system	NE, PE

Table 52: System Status Commands (Continued)

Command	Function	Mode
<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, the number of free entries, and the overall percentage of TCAM in use.

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
  Total Policy Control Entries : 1024
  Free Policy Control Entries  : 836
  Entries Used by System       : 188
  Entries Used by User         : 0
  TCAM Utilization              : 18.35%
Console#
```

show memory This command shows memory utilization parameters.

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, and the total amount of system memory.

EXAMPLE

```
Console#show memory
Status Bytes      %
-----
Free   138711040  51
Used   129724416  49
Total   268435456
```

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

```
Console#
```

RELATED COMMANDS

[memory \(803\)](#)

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

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 18%

CPU Utilization in the past 60 seconds
Average Utilization      : 16%
Maximum Utilization      : 19%

Alarm Status
Current Alarm Status     : Off
Last Alarm Start Time    : Sep 26 01:39:04 2011
Last Alarm Duration Time : 4 seconds

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

Console#
```

RELATED COMMANDS

[process cpu \(804\)](#)

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: 1-28/52)

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

vlan *vlan-id* (Range: 1-4093)

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 the switch
 - 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
 - Interface settings
 - Any configured settings for the console port and Telnet

EXAMPLE

```
Console#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_00</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
VLAN 1 name DefaultVlan media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
switchport allowed vlan add 4093 tagged
:
!
interface vlan 1
ip address dhcp
ip dhcp client class-id text Edge-Core
!
```

```
line console
!  
line vty
!  
end
!  
Console#
```

RELATED COMMANDS[show startup-config \(729\)](#)

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 the switch
 - 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 \(727\)](#)

show system This command displays system information.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

- ◆ For a description of the items shown by this command, refer to ["Displaying System Information" on page 120](#) and ["Displaying Hardware/Software Versions" on page 121](#).
- ◆ No information will be displayed under POST Result, unless there is a problem with the unit. If any POST test indicates "FAIL," contact your distributor for assistance.

EXAMPLE

```
Console#show system
System Description : ECS4510-28T
System OID String : 1.3.6.1.4.1.259.10.1.24.1
System Information
  System Up Time      : 0 days, 8 hours, 13 minutes, and 38.59 seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 00-00-E8-94-40-00
  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 Fan:
  Force Fan Speed Full : Disabled
Unit 1
  Fan 1: Ok           Fan 2: Ok

System Temperature:
Unit 1
  Temperature 1: 39 degrees

Main Power Status      : Up
Redundant Power Status : Not present
Console#
```

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

```

Console#show tech-support
show system:
System Description : ECS4510-28T
System OID String  : 1.3.6.1.4.1.259.10.1.24.1
System Information
  System Up Time      : 0 days, 0 hours, 52 minutes, and 2.21 seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 00-E0-00-00-00-01
  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
  :

```

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
  steve                    15 None

Online Users:
  Line   User Name                Idle time (h:m:s) Remote IP addr
  -----
*console admin                0:00:00
VTY 0   admin                0:00:10 192.168.0.99
SSH 1   steve                0:00:06 192.168.1.19

Web Online Users:
  Line   User Name                Idle time (h:m:s) Remote IP Addr
  -----
  HTTP   admin                0:00:01 192.168.0.99
Console#

```

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

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

See ["Displaying Hardware/Software Versions" on page 121](#) for detailed information on the items displayed by this command.

EXAMPLE

```
Console#show version
Unit 1
  Serial Number       : S123456
  Hardware Version    : R0A
  EPLD Version        : R00 V0.04
  Number of Ports     : 28
  Main Power Status   : Up
  Redundant Power Status : Not present
  Role                : Master
  Loader Version      : 0.0.0.10
  Linux Kernel Version : 2.6.22.18
  Boot ROM Version    : 0.0.0.1
  Operation Code Version : 1.3.1.4
```

```
Console#
```

show watchdog This command shows if watchdog debugging is enabled.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show watchdog

Software Watchdog Information
  Status : 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
Console#
```

FRAME SIZE

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

Table 53: Frame Size Commands

Command	Function	Mode
jumbo frame	Enables support for jumbo frames	GC

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

SYNTAX

[no] jumbo frame

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

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

EXAMPLE

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

RELATED COMMANDS

[show system \(729\)](#)

[show ipv6 mtu \(1390\)](#)

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/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/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/TFTP server, but cannot be used as the destination on the switch.

Table 54: Flash/File Commands

Command	Function	Mode
<i>General Commands</i>		
boot system	Specifies the file or image used to start up the system	GC
copy	Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server	PE
delete	Deletes a file or code image	PE
dir	Displays a list of files in flash memory	PE
whichboot	Displays the files booted	PE
<i>Automatic Code Upgrade Commands</i>		
upgrade opcode auto	Automatically upgrades the current image when a new version is detected on the indicated server	GC

Table 54: Flash/File Commands (Continued)

Command	Function	Mode
upgrade opcode path	Specifies an FTP/TFTP server and directory in which the new opcode is stored	GC
upgrade opcode reload	Reloads the switch automatically after the opcode upgrade is completed	GC
show upgrade	Shows the opcode upgrade configuration settings.	PE
<i>TFTP Configuration Commands</i>		
ip tftp retry	Specifies the number of times the switch can retry transmitting a request to a TFTP server	GC
ip tftp timeout	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
show ip tftp	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 {**boot-rom** | **config** | **opcode**}: *filename*

boot-rom* - Boot ROM.

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 \(739\)](#)

[whichboot \(740\)](#)

copy This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/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/TFTP server and the quality of the network connection.

SYNTAX

```
copy file {file | ftp | running-config | startup-config | tftp}  
copy running-config {file | ftp | startup-config | tftp}  
copy startup-config {file | ftp | running-config | tftp}  
copy tftp {file | https-certificate | public-key |  
running-config | startup-config}
```

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 852.](#))

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

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 128 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/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" on page 338](#). For information on configuring the switch to use HTTPS for a secure connection, see the [ip http secure-server](#) command.
- ◆ 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.

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#
```

delete This command deletes a file or image.

SYNTAX

delete *filename*

filename - Name of configuration file or code image.

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.

EXAMPLE

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

```
Console#delete test2.cfg
Console#
```

RELATED COMMANDS

[dir \(739\)](#)

[delete public-key \(858\)](#)

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

SYNTAX

dir {**boot-rom** | **config** | **opcode**}: [*filename*]

boot-rom - Boot ROM (or diagnostic) image file.

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 55: File Directory Information

Column Heading	Description
File Name	The name of the file.
File Type	File types: Boot-Rom, 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	Modify Time	Size(bytes)		

ECS4510-28T_V1.1.2.1.bix	OpCode	N	2012-03-30 03:03:17	13366912		
ECS4510-28T_V1.3.1.4.bix	OpCode	Y	2012-08-09 09:39:38	14145476		
Factory_Default_Config.cfg	Config	N	2012-03-09 05:37:42	455		
startup1.cfg	Config	Y	2012-03-30 02:41:56	1611		

Free space for compressed user config files:				56287232		
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	Modify	Time	Size (bytes)

Unit 1:					
ECS4510-28T_V1.3.1.4.bix	OpCode	Y	2012-08-09	09:39:38	14145476
startup1.cfg	Config	Y	2012-03-30	02:41:56	161
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 ECS4510-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 ECS4510-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    : ECS4510-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 56: Line Commands

Command	Function	Mode
line	Identifies a specific line for configuration and starts the line configuration mode	GC
accounting commands	Applies an accounting method to commands entered at specific CLI privilege levels	LC
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	LC
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	LC
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC
login	Enables password checking at login	LC
parity*	Defines the generation of a parity bit	LC
password	Specifies a password on a line	LC
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC
silent-time*	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	LC
speed*	Sets the terminal baud rate	LC
stopbits*	Sets the number of the stop bits transmitted per byte	LC
timeout login response	Sets the interval that the system waits for a login attempt	LC
disconnect	Terminates a line connection	PE
terminal	Configures terminal settings, including escape-character, line length, terminal type, and width	PE
show line	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 \(756\)](#)

[show users \(731\)](#)

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

RELATED COMMANDS

[parity \(750\)](#)

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


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

RELATED COMMANDS

[username \(825\)](#)

[password \(750\)](#)

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

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 during system bootup or when downloading the configuration file from an FTP/TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

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

RELATED COMMANDS[login \(749\)](#)[password-thresh \(751\)](#)

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

RELATED COMMANDS

[silent-time \(752\)](#)

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

RELATED COMMANDS

[password-thresh \(751\)](#)

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

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

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 \(861\)](#)[show users \(731\)](#)

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: 0-512, 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 57: Event Logging Commands

Command	Function	Mode
<code>logging facility</code>	Sets the facility type for remote logging of syslog messages	GC
<code>logging history</code>	Limits syslog messages saved to switch memory based on severity	GC
<code>logging host</code>	Adds a syslog server host IP address that will receive logging messages	GC
<code>logging on</code>	Controls logging of error messages	GC
<code>logging trap</code>	Limits syslog messages saved to a remote server based on severity	GC
<code>clear log</code>	Clears messages from the logging buffer	PE
<code>show log</code>	Displays log messages	PE
<code>show logging</code>	Displays the state of logging	PE

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 58: 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

[no] logging host *host-ip-address* [**port** *udp-port*]

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

udp-port - Host UDP port to use. (Range: 1-65535; Default: 514)

DEFAULT SETTING

None

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 \(758\)](#)
[logging trap \(760\)](#)
[clear log \(760\)](#)

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 758](#). 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 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 \(761\)](#)

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 {flash | ram | sendmail | trap}

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 766](#)).

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
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
Console#
```

Table 59: show logging flash/ram - display description

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

The following example displays settings for the trap function.

```
Console#show logging trap
Remote Log Status          : Disabled
Remote Log Facility Type   : Local use 7
Remote Log Level Type      : Debugging messages
```

```

Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Console#

```

Table 60: show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
REMOTELOG status	Shows if remote logging has been enabled via the logging trap command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the logging facility command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.
REMOTELOG server IP address	The address of syslog servers as specified in the logging host command.

RELATED COMMANDS

[show logging sendmail \(766\)](#)

SMTP ALERTS

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

Table 61: Event Logging Commands

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

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

SYNTAX

[no] logging sendmail

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

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

logging sendmail 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 or IPv6 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 758](#)). 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 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 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

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show logging sendmail
SMTP servers
-----
192.168.1.19
```

```

SMTP Minimum Severity Level: 7

SMTP destination email 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 62: 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
<i>Manual Configuration Commands</i>		
<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

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 (i.e., 00:00:00, Jan. 1, 2001).
- ◆ 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 2002
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 \(769\)](#)

[sntp poll \(769\)](#)

[show sntp \(770\)](#)

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 \(768\)](#)

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 an 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)#ntp server 10.1.0.19
Console#
```

RELATED COMMANDS

[ntp client \(768\)](#)

[ntp poll \(769\)](#)

[show ntp \(770\)](#)

show ntp 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 ntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
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#
```

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 \(771\)](#)

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 \(770\)](#)

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 (i.e., 00:00:00, Jan. 1, 2001).
- ◆ 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 \(768\)](#)

[ntp server \(773\)](#)

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 \(772\)](#)

[show ntp \(774\)](#)

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 2011
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 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 (west) of UTC.

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

EXAMPLE

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

RELATED COMMANDS

[show sntp \(770\)](#)

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, 2011.

```
Console#calendar set 15:12:34 1 February 2011
Console#
```

show calendar This command displays the system clock.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show calendar
15:12:34 February 1 2011
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 63: Time Range Commands

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

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

SYNTAX

[no] time-range *name*

name - Name of the time range. (Range: 1-16 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.

EXAMPLE

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

RELATED COMMANDS

[Access Control Lists \(949\)](#)

absolute This command sets the 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: 2009-2109)

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: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show time-range r&d
Time-range r&d:
  absolute start 01:01 01 April 2009
  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 64: Switch Cluster Commands

Command	Function	Mode
cluster	Configures clustering on the switch	GC
cluster commander	Configures the switch as a cluster Commander	GC
cluster ip-pool	Sets the cluster IP address pool for Members	GC
cluster member	Sets Candidate switches as cluster members	GC
rcommand	Provides configuration access to Member switches	GC
show cluster	Displays the switch clustering status	PE
show cluster members	Displays current cluster Members	PE
show cluster candidates	Displays current cluster Candidates in the network	PE

Using Switch Clustering

- ◆ A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and

then use the Commander to manage the Member switches through the cluster's "internal" IP addresses.

- ◆ Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- ◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.



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 enabled), 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 Commander 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  : ECS4510-28T
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
-----
Active member  00-E0-0C-00-00-FE  ECS4510-28T
CANDIDATE      00-12-CF-0B-47-A0  ECS4510-28T
Console#
```

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 65: 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
<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
<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

Table 65: SNMP Commands (Continued)

Command	Function	Mode
<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>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>show memory</code>	Shows memory utilization parameters	PE
<code>show process cpu</code>	Shows CPU utilization parameters	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 \(788\)](#)

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 \(788\)](#)

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
  Link-up-down   : Enabled

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 | link-up-down | ethernet cfm]

authentication - Keyword to issue authentication failure notifications.

link-up-down - Keyword to issue link-up or link-down notifications.

ethernet cfm - Connectivity Fault Management traps. For more information on these traps, see ["CFM Commands" on page 1295](#).

DEFAULT SETTING

Issue authentication and link-up-down traps.

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 and link-up-down 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, link-up, and link-down 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 link-up-down
Console(config)#
```

RELATED COMMANDS

[snmp-server host \(791\)](#)

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" on page 442](#) 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 787](#)).
2. Create a view with the required notification messages ([page 797](#)).
3. Create a group that includes the required notify view ([page 794](#)).
4. Allow the switch to send SNMP traps; i.e., notifications ([page 790](#)).
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 787](#)).
 2. Create a local SNMPv3 user to use in the message exchange process ([page 795](#)).
 3. Create a view with the required notification messages ([page 797](#)).
 4. Create a group that includes the required notify view ([page 794](#)).
 5. Allow the switch to send SNMP traps; i.e., notifications ([page 790](#)).
 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 \(790\)](#)

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 - The Internet address of the remote device.

engineid-string - String identifying the engine ID. (Range: 1-26 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 795](#)).

EXAMPLE

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engineID remote 9876543210 192.168.1.19
Console(config)#
```

RELATED COMMANDS

[snmp-server host](#) ([791](#))

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](#)" on [page 442](#) 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: public²⁴ (read only), private²⁵ (read/write)

readview - Every object belonging to the Internet OID space (1).

writeview - Nothing is defined.

notifyview - Nothing is defined.

COMMAND MODE

Global Configuration

²⁴. No view is defined.

²⁵. Maps to the defaultview.

COMMAND USAGE

- ◆ A group sets the access policy for the assigned users.
- ◆ When authentication is selected, the MD5 or SHA algorithm is used as specified in the [snmp-server user](#) command.
- ◆ When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- ◆ For additional information on the notification messages supported by this switch, see [Table 31, "Supported Notification Messages," on page 452](#). 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* [**remote** *ip-address*]
 {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*
 [**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

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 - The Internet address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

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. (A minimum of eight characters is required.)

priv 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.

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 group r&d v3 auth md5 greenpeace priv  
des56 einstien  
Console(config)#snmp-server user mark group 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 this 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 EngineID                               IP address
80000000030004e2b316c54321                         192.168.1.19
Console#
```

Table 66: 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
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
```

```

Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#

```

Table 67: show snmp group - display description

Field	Description
Group Name	Name of an SNMP group.
Security Model	The SNMP version.
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
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 68: 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.
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 69: 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

Enabled

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 - The Internet 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 be exceeding 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 \(726\)](#)

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 \(727\)](#)

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 70: 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

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28

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 757](#)).

trap – Sends a trap message to all configured trap managers (see ["snmp-server host" on page 791](#)).

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: 1-127 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*
 [[**owner** *name*] [**buckets** *number*] [**interval** *seconds*]] |
 [**buckets** *number*] [**interval** *seconds*] | **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: 1-127 characters)

DEFAULT SETTING

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28

Buckets: 50

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 This command enables the collection of statistics on a physical interface.
rmon1 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: 1-127 characters)

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- ◆ The information collected for each entry includes:
 input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

EXAMPLE

```

Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlentry 1 owner mike
Console(config-if)#

```

show rmon alarms This command shows the settings for all configured alarms.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show rmon alarms
Alarm 1 is valid, owned by
Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
Taking delta samples, last value was 0
Rising threshold is 892800, assigned to event 0
Falling threshold is 446400, assigned to event 0
:

```

show rmon events This command shows the settings for all configured events.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show rmon events
Event 2 is valid, owned by mike
Description is urgent
Event firing causes log and trap to community , last fired 00:00:00
Console#

```

show rmon history This command shows the sampling parameters configured for each entry in the history group.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show rmon history
Entry 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
Requested # of time intervals, ie buckets, is 8
Granted # of time intervals, ie buckets, is 8
Sample # 1 began measuring at 00:00:01
Received 77671 octets, 1077 packets,
61 broadcast and 978 multicast packets,

```



```

0 undersized and 0 oversized packets,
0 fragments and 0 jabbers packets,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Network utilization is estimated at 0
:

```

show rmon statistics This command shows the information collected for all configured entries in the statistics group.

COMMAND MODE
Privileged Exec

EXAMPLE

```

Console#show rmon statistics
Interface 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
Received 164289 octets, 2372 packets,
120 broadcast and 2211 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events (due to lack of resources): 0
# of packets received of length (in octets):
64: 2245, 65-127: 87, 128-255: 31,
256-511: 5, 512-1023: 2, 1024-1518: 2
:

```


Flow sampling (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.

Table 71: sFlow Commands

Command	Function	Mode
<code>sflow</code>	Enables sFlow globally for the switch	GC
<code>sflow destination</code>	Configures the IP address and UDP port used by the Collector	IC
<code>sflow max-datagram-size</code>	Configures the maximum size of the sFlow datagram payload	IC
<code>sflow max-header-size</code>	Configures the maximum size of the sFlow datagram header	IC
<code>sflow owner</code>	Configures the name of the receiver	IC
<code>sflow polling-interval</code>	Configures the interval at which counters are added to the sample datagram	IC
<code>sflow sample</code>	Configures the packet sampling rate	IC
<code>sflow source</code>	Enables sFlow on the source ports to be monitored	IC
<code>sflow timeout</code>	Configures the length of time samples are sent to the Collector before resetting all sFlow port parameters	IC
<code>show sflow</code>	Shows the global and interface settings for the sFlow process	PE

sflow This command enables sFlow globally for the switch. Use the **no** form to disable this feature.

SYNTAX

[no] sflow

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Flow sampling must be enabled globally on the switch, as well as for those ports where it is required (see the [sflow source](#) command).

EXAMPLE

```
Console(config)#sflow
Console(config)#
```

sflow destination This command configures the IP address and UDP port used by the Collector. Use the **no** form to restore the default settings.

SYNTAX

sflow destination {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}
[*destination-udp-port*]

no sflow destination

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: 0-65534)

DEFAULT SETTING

IP Address: null

UDP Port: 6343

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example configures the Collector's IP address, and uses the default UDP port.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

sflow max-datagram-size This command configures the maximum size of the sFlow datagram payload. Use the **no** form to restore the default setting.

SYNTAX

sflow max-datagram-size *max-datagram-size*

no max-datagram-size

max-datagram-size - The maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)

DEFAULT SETTING

1400 bytes

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

sflow max-header-size This command configures the maximum size of the sFlow datagram header. Use the **no** form to restore the default setting.

SYNTAX

sflow max-header-size *max-header-size*

no max-header-size

max-header-size - The maximum size of the sFlow datagram header. (Range: 64-256 bytes)

DEFAULT SETTING

128 bytes

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

sflow owner This command configures the name of the receiver (i.e., sFlow Collector). Use the **no** form to remove this name.

SYNTAX

sflow owner *name*

no sflow owner

name - The name of the receiver. (Range: 1-256 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example set the owner's name to Lamar.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow owner Lamar
Console(config-if)#
```

sflow polling-interval This command configures the interval at which counters are added to the sample datagram. Use the **no** form to restore the default polling interval.

SYNTAX

sflow polling-interval *seconds*

no sflow polling-interval

seconds - The interval at which the sFlow process adds counter values to the sample datagram. (Range: 0-10,000,000 seconds, where 0 disables this feature)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

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 sample This command configures the packet sampling rate. Use the **no** form to restore the default rate.

SYNTAX

sflow sample *rate*

no sflow sample

rate - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 256-16777215 packets)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example sets the sample rate to 1 out of every 100 packets.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow sample 100
Console(config-if)#
```

sflow source This command enables sFlow on the source ports to be monitored. Use the **no** form to disable sFlow on the specified ports.

SYNTAX

[no] sflow source

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example enables flow control on ports 9 through 16.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow source
Console(config-if)#
```

sflow timeout This command configures the length of time samples are sent to the Collector before resetting all sFlow port parameters. Use the **no** form to restore the default time out.

SYNTAX

sflow timeout *seconds*

no sflow timeout

seconds - The length of time the sFlow process continuously sends samples to the Collector before resetting all sFlow port parameters. (Range: 0-10000000 seconds, where 0 indicates no time out)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

The sFlow agent sends sample data to an sFlow collector until the timeout set by this command expires. The sFlow agent then resets the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.

EXAMPLE

This example sets the time out to 1000 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

show sflow This command shows the global and interface settings for the sFlow process.

SYNTAX

show sflow interface [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

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

COMMAND MODE
Privileged Exec**EXAMPLE**

```
Console#show sflow interface ethernet 1/9
```

```
Interface of Ethernet 1/9 :  
  Interface status      : Enabled  
  Owner name            : Lamar  
  Owner destination     : 192.168.0.4  
  Owner socket port     : 6343  
  Time out              : 9994  
  Maximum header size   : 256  
  Maximum datagram size : 1500  
  Sample rate           : 1/256  
  Polling interval      : 10
```

```
Console#
```


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 access²⁶ to the data ports.

Table 72: Authentication Commands

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

26. For other methods of controlling client access, see ["General Security Measures" on page 887](#).

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 746](#)), user authentication via a remote authentication server ([page 823](#)), and host access authentication for specific ports ([page 862](#)).

Table 73: User Access Commands

Command	Function	Mode
enable password	Sets a password to control access to the Privileged Exec level	GC
username	Establishes a user name-based authentication system at login	GC
privilege	Assigns a privilege level to specified command groups or individual commands	GC
show privilege	Shows the privilege level for the current user, or the privilege level for commands modified by the privilege command	PE

enable password After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

SYNTAX

enable password [**level** *level*] {**0** | **7**} *password*

no enable password [**level** *level*]

level *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)

{**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 or when downloading the configuration file from a TFTP server. 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 \(709\)](#)

[authentication enable \(828\)](#)

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)

access-level *level* - Specifies the user level.

The device has two predefined privilege levels:

0: Normal Exec, **15**: Privileged Exec.

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 Normal Exec.

The factory defaults for the user names and passwords are:

Table 74: 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 or when downloading the configuration file from an FTP/TFTP server. 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 698](#) and ["Configuration Commands" on page 700](#).)

all - Modifies the privilege level for all subcommands under the specified *command*.

level *level* - Specifies the privilege level for the specified *command*.

This device has three predefined privilege levels: **0**: Normal Exec, **8**: Manager, **15**: Privileged Exec. (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 75: Authentication Sequence Commands

Command	Function	Mode
authentication enable	Defines the authentication method and precedence for command mode change	GC
authentication login	Defines logon authentication method and precedence	GC

authentication enable This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command. Use the **no** form to restore the default.

SYNTAX

authentication enable {[local] [radius] [tacacs]}

no authentication enable

local - Use local password only.

radius - Use RADIUS server password only.

tacacs - Use TACACS server password.

DEFAULT SETTING

Local

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- ◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- ◆ You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

EXAMPLE

```
Console(config)#authentication enable radius
Console(config)#
```

RELATED COMMANDS

enable password - sets the password for changing command modes (824)

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 (825)

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 76: RADIUS Client Commands

Command	Function	Mode
<code>radius-server acct-port</code>	Sets the RADIUS server network port	GC
<code>radius-server auth-port</code>	Sets the RADIUS server network port	GC
<code>radius-server host</code>	Specifies the RADIUS server	GC
<code>radius-server key</code>	Sets the RADIUS encryption key	GC
<code>radius-server retransmit</code>	Sets the number of retries	GC
<code>radius-server timeout</code>	Sets the interval between sending authentication requests	GC
<code>show radius-server</code>	Shows the current RADIUS settings	PE

radius-server acct-port This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

SYNTAX

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

DEFAULT SETTING

1813

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server acct-port 181
Console(config)#
```

radius-server auth-port This command sets the RADIUS server network port. Use the **no** form to restore the default.

SYNTAX

radius-server auth-port *port-number*

no radius-server auth-port

port-number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

DEFAULT SETTING

1812

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server host This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

SYNTAX

[no] radius-server index host *host-ip-address* [**acct-port** *acct-port*] [**auth-port** *auth-port*] [**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. Do not use blank spaces in the string. (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. Do not use blank spaces in the string. (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 77: TACACS+ Client Commands

Command	Function	Mode
<code>tacacs-server host</code>	Specifies the TACACS+ server and optional parameters	GC
<code>tacacs-server key</code>	Sets the TACACS+ encryption key	GC
<code>tacacs-server port</code>	Specifies the TACACS+ server network port	GC
<code>tacacs-server retransmit</code>	Sets the number of retries	GC
<code>tacacs-server timeout</code>	Sets the interval between sending authentication requests	GC
<code>show tacacs-server</code>	Shows the current TACACS+ settings	GC

tacacs-server host This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

SYNTAX

```

tacacs-server index host host-ip-address [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. Do not use blank spaces in the string. (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. Do not use blank spaces in the string. (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 78: AAA Commands

Command	Function	Mode
<code>aaa accounting commands</code>	Enables accounting of Exec mode commands	GC
<code>aaa accounting dot1x</code>	Enables accounting of 802.1X services	GC
<code>aaa accounting exec</code>	Enables accounting of Exec services	GC
<code>aaa accounting update</code>	Enables periodic updates to be sent to the accounting server	GC
<code>aaa authorization exec</code>	Enables authorization of Exec sessions	GC
<code>aaa group server</code>	Groups security servers in to defined lists	GC
<code>server</code>	Configures the IP address of a server in a group list	SG
<code>accounting dot1x</code>	Applies an accounting method to an interface for 802.1X service requests	IC
<code>accounting commands</code>	Applies an accounting method to CLI commands entered by a user	Line
<code>accounting exec</code>	Applies an accounting method to local console, Telnet or SSH connections	Line
<code>authorization exec</code>	Applies an authorization method to local console, Telnet or SSH connections	Line
<code>show accounting</code>	Displays all accounting 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 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 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: 1-28/52)

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#

```

WEB SERVER

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

Table 79: Web Server Commands

Command	Function	Mode
<code>ip http port</code>	Specifies the port to be used by the web browser interface	GC
<code>ip http server</code>	Allows the switch to be monitored or configured from a browser	GC
<code>ip http secure-port</code>	Specifies the UDP port number for HTTPS	GC
<code>ip http secure-server</code>	Enables HTTPS (HTTP/SSL) for encrypted communications	GC

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 \(848\)](#)

[show system \(729\)](#)

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 port \(847\)](#)

[show system \(729\)](#)

ip http secure-port This command specifies the UDP 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 UDP 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 \(849\)](#)
[show system \(729\)](#)

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 6.x or above, and Mozilla Firefox 3.6.2/4/5.

The following web browsers and operating systems currently support HTTPS:

Table 80: HTTPS System Support

Web Browser	Operating System
Internet Explorer 6.x or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7
Mozilla Firefox 3.6.2/4/5	Windows 2000, Windows XP, Linux

- ◆ To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 338. Also refer to the [copy tftp https-certificate](#) command.

EXAMPLE

```
Console(config)#ip http secure-server
Console(config)#
```

RELATED COMMANDS

[ip http secure-port \(848\)](#)
[copy tftp https-certificate \(736\)](#)
[show system \(729\)](#)

TELNET SERVER

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

Table 81: Telnet Server Commands

Command	Function	Mode
ip telnet max-sessions	Specifies the maximum number of Telnet sessions that can simultaneously connect to this system	GC
ip telnet port	Specifies the port to be used by the Telnet interface	GC
ip telnet server	Allows the switch to be monitored or configured from Telnet	GC
show ip telnet	Displays configuration settings for the Telnet server	PE



NOTE: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

ip telnet max-sessions This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** form to restore the default setting.

SYNTAX

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count - The maximum number of allowed Telnet session.
(Range: 0-8)

DEFAULT SETTING

8 sessions

COMMAND MODE

Global Configuration

COMMAND USAGE

A maximum of eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number of eight sessions).

EXAMPLE

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

ip telnet port This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

SYNTAX

ip telnet port *port-number*

no telnet port

port-number - The TCP port number to be used by the browser interface. (Range: 1-65535)

DEFAULT SETTING

23

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip telnet port 123
Console(config)#
```

ip telnet server This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

SYNTAX

[no] ip telnet server

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip telnet server
Console(config)#
```

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 82: Secure Shell Commands

Command	Function	Mode
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC
ip ssh server	Enables the SSH server on the switch	GC
ip ssh server-key size	Sets the SSH server key size	GC

Table 82: Secure Shell Commands (Continued)

Command	Function	Mode
<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
<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
10825913212890233765468017262725714134287629413011961955667825
95664104869574278881462065194174677298486546861571773939016477
```

```
93559423035774130980227370877945452408397175264635805817671670
9574804776117
```

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
13410816856098939210409449201554253476316419218729589211431738
80055536161631051775940838686311092912322268285192543746031009
37187721199696317813662774141689851320491172048303392543241016
37997592371449011938006090253948408482717819437228840253311595
2134861022902978982721353267131629432532818915045306393916643
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-retires 2  
Console(config)#
```

RELATED COMMANDS

[show ip ssh \(860\)](#)

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 \(858\)](#)
[show ssh \(861\)](#)

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

10 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 \(748\)](#)

[show ip ssh \(860\)](#)

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 \(859\)](#)
[ip ssh save host-key \(860\)](#)

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 \(858\)](#)
[ip ssh save host-key \(860\)](#)
[no ip ssh server \(856\)](#)

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 \(858\)](#)

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: 1-8 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 AAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PATp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKx15fwFfv
JlPdOkFgzLGMInvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMacNBPjBrRAAAAFQChb4vsdfQGNIjwbv
wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wy4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395Nly5Qd7ZDxfA9mCOFT/yyEfbbobMJZi8oGCstSN0xrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#

```

show ssh This command displays the current SSH server connections.

COMMAND MODE
Privileged Exec**EXAMPLE**

```

Console#show ssh
Connection Version State Username Encryption
0 2.0 Session-Started admin ctos aes128-cbc-hmac-md5
stoc aes128-cbc-hmac-md5
Console#

```

Table 83: show ssh - display description

Field	Description
Connection	The session number. (Range: 0-3)
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 84: 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 eapol-pass-through</code>	Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled	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

Table 84: 802.1X Port Authentication Commands (Continued)

Command	Function	Mode
<i>Supplicant Commands</i>		
<code>dot1x identity profile</code>	Configures dot1x supplicant user name and password	GC
<code>dot1x max-start</code>	Sets the maximum number of times that a port supplicant will send an EAP start frame to the client	IC
<code>dot1x pae supplicant</code>	Enables dot1x supplicant mode on an interface	IC
<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
<code>dot1x timeout start-period</code>	Sets the time that a supplicant port waits before resending an EAPOL start frame to the 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 global and port settings to their default values.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dot1x default
Console(config)#
```

dot1x eapol-pass-through This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the **no** form to restore the default.

SYNTAX

[no] dot1x eapol-pass-through

DEFAULT SETTING

Discards all EAPOL frames when dot1x is globally disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the **dot1x eapol pass-through** command can be used to forward EAPOL frames from

other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

- ◆ When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the **no dot1x eapol-pass-through** command can be used to discard unnecessary EAPOL traffic.

EXAMPLE

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

```
Console(config)#dot1x eapol-pass-through
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).

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 (868)`

`dot1x timeout quiet-period`

This command sets the time that a switch port waits after the maximum request count (see [page 865](#)) 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: 1-28/52)

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 identity profile This command sets the dot1x supplicant user name and password. Use the **no** form to delete the identity settings.

SYNTAX

dot1x identity profile {**username** *username* | **password** *password*}

no dot1x identity profile {**username** | **password**}

username - Specifies the supplicant user name.
(Range: 1-8 characters)

password - Specifies the supplicant password.
(Range: 1-8 characters)

DEFAULT

No user name or password

COMMAND MODE

Global Configuration

COMMAND USAGE

The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see the [dot1x pae supplicant](#) command on [page 872](#)).

EXAMPLE

```
Console(config)#dot1x identity profile username steve
Console(config)#dot1x identity profile password excess
Console(config)#
```

dot1x max-start This command sets the maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. Use the **no** form to restore the default value.

SYNTAX

dot1x max-start *count*

no dot1x max-start

count - Specifies the maximum number of EAP start frames.
(Range: 1-65535)

DEFAULT

3

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-start 10
Console(config-if)#
```

dot1x pae supplicant This command enables dot1x supplicant mode on a port. Use the **no** form to disable dot1x supplicant mode on a port.

SYNTAX

[no] **dot1x pae supplicant**

DEFAULT

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- ◆ When devices attached to a port must submit requests to another authenticator on the network, configure the identity profile parameters (see [dot1x identity profile](#) command on [page 871](#)) which identify this switch as a supplicant, and enable dot1x supplicant mode for those ports which must authenticate clients through a remote authenticator using this command. In this mode the port will not respond to dot1x messages meant for an authenticator.
- ◆ This switch can be configured to serve as the authenticator on selected ports by setting the control mode to "auto" (see the [dot1x port-control](#) command on [page 867](#)), and as a supplicant on other ports by the setting the control mode to "force-authorized" and enabling dot1x supplicant mode with this command.
- ◆ A port cannot be configured as a dot1x supplicant if it is a member of a trunk or LACP is enabled on the port.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x pae supplicant
Console(config-if)#
```

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 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)#
```

dot1x timeout start-period This command sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator. Use the **no** form to restore the default setting.

SYNTAX

dot1x timeout start-period *seconds*

no dot1x timeout start-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 start-period 60
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: 1-28/52)

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 864](#)).
- ◆ *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled ([page 863](#)).

- ◆ *Supplicant Parameters* – Shows the supplicant user name used when the switch responds to an MD5 challenge from an authenticator ([page 871](#)).
- ◆ *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 866](#)).
 - Control Mode – Dot1x port control mode ([page 867](#)).
 - 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 867](#)).
 - Reauth Period – Time after which a connected client must be re-authenticated ([page 868](#)).
 - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client ([page 868](#)).
 - TX Period – Time a port waits during authentication session before re-transmitting EAP packet ([page 870](#)).
 - 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 865](#)).
 - 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 867](#)).
 - Intrusion Action– Shows the port response to intrusion when authentication fails ([page 864](#)).
 - 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

Supplicant Parameters:
  Identity Profile Username : steve

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 1/27 Disabled    Single-Host    Force-Authorized  Yes
Eth 1/28 Enabled      Single-Host    Auto              Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1
802.1X Supplicant is disabled on port 1/1
.
.
802.1X Authenticator is enabled on port 28
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 85: 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. 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

- ◆ 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 reenter 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 86: 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 and generic error message 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 or remote-id 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
<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 and generic error message for the switch. Use the **no** form to restore the default settings.

SYNTAX

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

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

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.

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 or remote-id for an interface. Use the **no** form to restore the default settings.

SYNTAX

pppoe intermediate-agent port-format-type {circuit-id | remote-id} *id-string*

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

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

DEFAULT SETTING

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

remote-id: port MAC address

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.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id
ECS4500-28
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: 1-28/52)
port-channel *channel-id* (Range: 1-16)

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: 1-28/52)

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

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 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
Oper Circuit-ID Oper Remote-ID
-----
Eth 1/2   Yes      Yes      Yes
1/2:vid   00-00-E8-94-40-02

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: 1-28/52)

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

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 87: show pppoe intermediate-agent statistics - display description

Field	Description
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

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 88: 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
IP Source Guard*	Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets
DoS Protection	Protects against Denial-of-Service attacks

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, DHCP Snooping, and then IP Source Guard.

PORT SECURITY

These commands can be used to enable port security on a port.

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 89: 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>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

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.

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 \(985\)](#)
[shutdown \(979\)](#)
[mac-address-table static \(1054\)](#)

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: 1-28/52)

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 90: show port security - display description

Field	Description
Port Security	The configured status (enabled or disabled).
Port Status	The operational status: <ul style="list-style-type: none"> Secure/Down – Port security is disabled. Secure/Up – Port security is enabled. Shutdown – Port is shut down due to a response to a port security violation.
Intrusion Action	The configured intrusion response.
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 port-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 ID : 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 ID : 2
  Last Intrusion MAC : 00-10-22-00-00-01
  Last Time Detected Intrusion MAC : 2010/7/29 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 91: 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 link-detection</code>	Enables the link detection feature	IC
<code>network-access link-detection link-down</code>	Configures the link detection feature to detect and act upon link-down events	IC
<code>network-access link-detection link-up</code>	Configures the link detection feature to detect and act upon link-up events	IC
<code>network-access link-detection link-up-down</code>	Configures the link detection feature to detect and act upon both link-up and link-down events	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 866](#)).
- ◆ The maximum number of secure MAC addresses supported for the switch system is 1024.

EXAMPLE

```
Console(config-if)#network-access aging
Console(config-if)#
```

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 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 92: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	service-policy-in = <i>policy-map-name</i>	service-policy-in=p1
Rate Limit	rate-limit-input = <i>rate</i>	rate-limit-input=100 (Kbps)
802.1p	switchport-priority-default = <i>value</i>	switchport-priority-default=2
IP ACL	ip-access-group-in = <i>ip-acl-name</i>	ip-access-group-in=ipv4acl
IPv6 ACL	ipv6-access-group-in = <i>ipv6-acl-name</i>	ipv6-access-group-in=ipv6acl
MAC ACL	mac-access-group-in = <i>mac-acl-name</i>	mac-access-group-in=macAcl

- ◆ When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- ◆ When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- ◆ While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.



NOTE: Any configuration changes for dynamic QoS are not saved to the switch configuration file.

EXAMPLE

The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

SYNTAX

[no] **network-access dynamic-vlan**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- ◆ When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch. 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 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: 1-4093)

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).

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access link-detection Use this command to enable link detection for the selected port. Use the **no** form of this command to restore the default.

SYNTAX

[no] network-access link-detection

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

network-access link-detection link- down

Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-down
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

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 the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link- up

Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-up
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

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 the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action trap
Console(config-if)#
```

network-access link-detection link- up-down

Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-up-down
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

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 the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
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: 0-2048; 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 trunk ports.

- ◆ 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: 1-28/52)

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: 1-28/52)

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: 1-28/52)

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 827](#)).

NOTE: Web authentication cannot be configured on trunk ports.

Table 93: Web Authentication

Command	Function	Mode
web-auth login-attempts	Defines the limit for failed web authentication login attempts	GC
web-auth quiet-period	Defines the amount of time to wait after the limit for failed login attempts is exceeded.	GC
web-auth session-timeout	Defines the amount of time a session remains valid	GC
web-auth system-auth-control	Enables web authentication globally for the switch	GC
web-auth	Enables web authentication for an interface	IC
web-auth re-authenticate (Port)	Ends all web authentication sessions on the port and forces the users to re-authenticate	PE
web-auth re-authenticate (IP)	Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate	PE
show web-auth	Displays global web authentication parameters	PE
show web-auth interface	Displays interface-specific web authentication parameters and statistics	PE
show web-auth summary	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: 1-28/52)

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: 1-28/52)

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: 1-28/52)

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 94: 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 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>	Specifies DHCP Option 82 circuit-id suboption information	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

Table 94: DHCP Snooping Commands (Continued)

Command	Function	Mode
<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 (917)`
`ip dhcp snooping trust (919)`

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 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 binding 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 \(912\)](#)
[ip dhcp snooping vlan \(917\)](#)
[ip dhcp snooping trust \(919\)](#)

**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: 1-4093)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ When DHCP snooping 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 \(912\)](#)
[ip dhcp snooping trust \(919\)](#)

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*

no dhcp snooping information option circuit-id

string - An arbitrary string inserted into the circuit identifier field.
(Range: 1-32 characters)

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 95: 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.

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 mv2
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 \(912\)](#)

[ip dhcp snooping vlan \(917\)](#)

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* **vlan** *vlan-id*]

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

vlan-id - ID of a configured VLAN (Range: 1-4093)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console(config)#
```

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#clear ip dhcp snooping database flash
Console(config)#
```

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(config)#ip dhcp snooping database flash
Console(config)#
```

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: enabled
DHCP Snooping Information Option Status: enabled
DHCP Snooping Information Option Sub-option Format: extra subtype included
DHCP Snooping Information Option Remote ID: MAC Address (ascii encoded)
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
  1,
Verify Source MAC-Address: enabled
Interface      Trusted      Circuit-ID Value
-----
Eth 1/1        Yes         park 19
Eth 1/2        No          ---
Eth 1/3        No          ---
Eth 1/4        No          ---
Eth 1/5        No          ---
.
.
.
```

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 96: DHCP Snooping Commands

Command	Function	Mode
ipv6 dhcp snooping	Enables DHCPv6 snooping globally	GC
ipv6 dhcp snooping vlan	Enables DHCPv6 snooping on the specified VLAN	GC
ipv6 dhcp snooping max-binding	Sets the maximum number of entries which can be stored in the binding database for an interface	IC
ipv6 dhcp snooping trust	Configures the specified interface as trusted	IC
clear ipv6 dhcp snooping binding	Clears DHCPv6 snooping binding table entries from RAM	PE
clear ipv6 dhcp snooping database flash	Removes all dynamically learned snooping entries from flash memory.	PE
show ipv6 dhcp snooping	Shows the DHCPv6 snooping configuration settings	PE
show ipv6 dhcp snooping binding	Shows the DHCPv6 snooping binding table entries	PE
show ipv6 dhcp snooping statistics	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 (925)`
`ipv6 dhcp snooping trust (926)`

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: 1-4093)

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 DHCP6 snooping for VLAN 1.

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

RELATED COMMANDS

[ipv6 dhcp snooping \(922\)](#)

[ipv6 dhcp snooping trust \(926\)](#)

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 \(922\)](#)

[ipv6 dhcp snooping vlan \(925\)](#)

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 database flash

This command removes all dynamically learned snooping entries from flash memory.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console(config)#clear ipv6 dhcp snooping database flash
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 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#
```

IP SOURCE GUARD

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see ["DHCPv4 Snooping" on page 911](#)). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

Table 97: IP 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>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 binding table. Use the **no** form to remove a static entry.

SYNTAX

ip source-guard binding *mac-address* **vlan** *vlan-id* *ip-address*
interface ethernet *unit/port*

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

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4093)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1)

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

DEFAULT SETTING

No configured entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ 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 933](#)).
- ◆ 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.
- ◆ Static bindings are processed as follows:
 - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.
 - If there is an entry with 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 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.

EXAMPLE

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

```
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 \(931\)](#)
[ip dhcp snooping \(912\)](#)
[ip dhcp snooping vlan \(917\)](#)

ip source-guard This command configures the switch to filter inbound traffic based 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 ([page 930](#)) 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 DHCP snooping is disabled (see [page 912](#)), 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.
 - 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 \(930\)](#)
[ip dhcp snooping \(912\)](#)
[ip dhcp snooping vlan \(917\)](#)

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 max-binding *number*

no ip source-guard max-binding

number - The maximum number of IP 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 DHCP snooping and static entries set by the **ip source-guard** command.

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)#ip source-guard max-binding 1
Console(config-if)#
```

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  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 ip source-guard binding This command shows the source guard binding table.

SYNTAX

show ip source-guard binding [dhcp-snooping | static]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see [page 911](#))

static - Shows static entries configured with the **ip source-guard binding** command (see [page 930](#)).

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip source-guard binding
MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
11-22-33-44-55-66 192.168.0.99      0 Static           1 Eth 1/5
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 98: ARP Inspection Commands

Command	Function	Mode
ip arp inspection	Enables ARP Inspection globally on the switch	GC
ip arp inspection filter	Specifies an ARP ACL to apply to one or more VLANs	GC
ip arp inspection log-buffer logs	Sets the maximum number of entries saved in a log message, and the rate at these messages are sent	GC
ip arp inspection validate	Specifies additional validation of address components in an ARP packet	GC
ip arp inspection vlan	Enables ARP Inspection for a specified VLAN or range of VLANs	GC

Table 98: ARP Inspection Commands (Continued)

Command	Function	Mode
<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**]

arp-acl-name - Name of an ARP ACL.
(Maximum length: 16 characters)

vlan-id - VLAN ID. (Range: 1-4093)

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 364](#).
- ◆ 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)

seconds - The interval at which log messages are sent.
(Range: 0-86400)

DEFAULT SETTING

Message Number: 5

Interval: 1 second

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] [src-mac] | ip [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.

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: 1-4093)

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. (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           : 10 s
Log Message Number             : 1
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: 1-28/52)

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-id - VLAN ID. (Range: 1-4093)

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 99: DoS Protection Commands

Command	Function	Mode
<code>dos-protection echo-charge</code>	Protects against DoS echo/charge attacks	GC
<code>dos-protection smurf</code>	Protects against DoS smurf attacks	GC
<code>dos-protection tcp-flooding</code>	Protects against DoS TCP-flooding attacks	GC
<code>dos-protection tcp-null-scan</code>	Protects against DoS TCP-null-scan attacks	GC
<code>dos-protection tcp-syn-fin-scan</code>	Protects against DoS TCP-SYN/FIN-scan attacks	GC
<code>dos-protection tcp-xmas-scan</code>	Protects against DoS TCP-XMAS-scan attacks	GC
<code>dos-protection udp-flooding</code>	Protects against DoS UDP-flooding attacks	GC
<code>dos-protection win-nuke</code>	Protects against DoS WinNuke attacks	GC
<code>show dos-protection</code>	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 to disable this feature.

SYNTAX

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

no dos-protection echo-charge

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 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

Enabled

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 to disable this feature.

SYNTAX

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

no dos-protection tcp-flooding

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 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

Enabled

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 syn-fin-scan**

DEFAULT SETTING

Enabled

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

Enabled

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 to disable this feature.

SYNTAX

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

no dos-protection udp-flooding

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 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), causing 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 to disable this feature.

SYNTAX

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

no dos-protection udp-flooding

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 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#
```

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 100: 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 101: IPv4 ACL Commands

Command	Function	Mode
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs	GC
permit, deny	Filters packets matching a specified source IPv4 address	IPv4-STD-ACL
permit, deny	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
ip access-group	Binds an IPv4 ACL to a port	IC
show ip access-group	Shows port assignments for IPv4 ACLs	PE
show ip access-list	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, no spaces or other special 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 64 rules.

EXAMPLE

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

RELATED COMMANDS

[permit, deny \(951\)](#)

[ip access-group \(954\)](#)

[show ip access-list \(955\)](#)

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: 1-32 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 \(950\)](#)

[Time Range \(776\)](#)

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}
  [precedence precedence] [dscp dscp]
  [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}
  [precedence precedence] [dscp dscp]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp
  {any | source address-bitmask | host source}
  {any | destination address-bitmask | host destination}
  [precedence precedence] [dscp dscp]
  [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}
  [precedence precedence] [dscp dscp]
  [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.

precedence – IP precedence level. (Range: 0-7)

dscp – DSCP priority level. (Range: 0-63)

sport – Protocol²⁷ source port number. (Range: 0-65535)

dport – Protocol²⁷ destination port number. (Range: 0-65535)

port-bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

27. Includes TCP, UDP or other protocol types.

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

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.
- ◆ You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- ◆ 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”

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 \(950\)](#)
[Time Range \(776\)](#)

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** | **out**}
[**time-range** *time-range-name*] [**counter**]

no ip access-group *acl-name* {**in** | **out**}

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name – Name of the time range.
(Range: 1-16 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 \(955\)](#)
[Time Range \(776\)](#)

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#
```

RELATED COMMANDS

[ip access-group \(954\)](#)

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: 16 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 \(951\)](#)
[ip access-group \(954\)](#)

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 102: IPv6 ACL Commands

Command	Function	Mode
access-list ipv6	Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs	GC
permit, deny	Filters packets matching a specified source IPv6 address	IPv6-STD-ACL
permit, deny	Filters packets meeting the specified criteria, including source or destination IPv6 address, DSCP traffic class, or next header type	IPv6-EXT-ACL
show ipv6 access-list	Displays the rules for configured IPv6 ACLs	PE
ipv6 access-group	Adds a port to an IPv6 ACL	IC
show ipv6 access-group	Shows port assignments for 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 \(Standard IPv6 ACL\) \(957\)](#)[permit, deny \(Extended IPv6 ACL\) \(958\)](#)[ipv6 access-group \(961\)](#)[show ipv6 access-list \(960\)](#)**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: 1-16 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 \(956\)](#)

[Time Range \(776\)](#)

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]
[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]
```

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.

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, 0-8 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)

time-range-name - Name of the time range.
(Range: 1-16 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 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
```

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the next header is 43.”

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 next-header 43
Console(config-ext-ipv6-acl)#
```

RELATED COMMANDS

[access-list ipv6 \(956\)](#)

[Time Range \(776\)](#)

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: 16 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 \(Standard IPv6 ACL\) \(957\)](#)

[permit, deny \(Extended IPv6 ACL\) \(958\)](#)

[ipv6 access-group \(961\)](#)

ipv6 access-group This command binds a port to an IPv6 ACL. Use the **no** form to remove the port.

SYNTAX

ipv6 access-group *acl-name* {**in** | **out**}
[**time-range** *time-range-name*] [**counter**]

no ipv6 access-group *acl-name* {**in** | **out**}

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name – Name of the time range.
(Range: 1-16 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 \(960\)](#)

[Time Range \(776\)](#)

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 \(961\)](#)

MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. 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 103: MAC ACL Commands

Command	Function	Mode
access-list mac	Creates a MAC ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL
mac access-group	Binds a MAC ACL to a port	IC
show mac access-group	Shows port assignments for MAC ACLs	PE
show mac access-list	Displays the rules for configured MAC ACLs	PE

access-list mac This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

SYNTAX

[no] access-list mac *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special 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 \(963\)](#)
[mac access-group \(965\)](#)
[show mac access-list \(966\)](#)

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. Use the **no** form to remove a rule.

SYNTAX

```
{permit | deny}
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]
  [time-range time-range-name]

no {permit | deny}
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [vid vid vid-bitmask] [ethertype protocol [protocol-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}
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]
  [time-range time-range-name]

no {permit | deny} tagged-eth2
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]

{permit | deny} untagged-eth2
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [ethertype protocol [protocol-bitmask]]
  [time-range time-range-name]

no {permit | deny} untagged-eth2
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [ethertype protocol [protocol-bitmask]]
```

```
{permit | deny} tagged-802.3  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-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}  
  [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 source or destination address.

host – A specific MAC address.

source – Source MAC address.

destination – Destination MAC address range with bitmask.

*address-bitmask*²⁸ – Bitmask for MAC address (in hexadecimal format).

vid – VLAN ID. (Range: 1-4093)

*vid-bitmask*²⁸ – VLAN bitmask. (Range: 1-4095)

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

*protocol-bitmask*²⁸ – Protocol bitmask. (Range: 0-ffff hex.)

time-range-name – Name of the time range.
(Range: 1-16 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.

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

- ◆ 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

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 \(962\)](#)

[Time Range \(776\)](#)

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** | **out**}
[**time-range** *time-range-name*] [**counter**]

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name – Name of the time range.
(Range: 1-30 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 \(966\)](#)
[Time Range \(776\)](#)

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 \(965\)](#)

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: 16 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 \(963\)](#)
[mac access-group \(965\)](#)

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 ([page 939](#)).

Table 104: ARP ACL Commands

Command	Function	Mode
access-list arp	Creates a ARP ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source or destination address in ARP messages	ARP-ACL
show access-list arp	Displays the rules for configured ARP ACLs	PE

access-list arp This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

SYNTAX

[no] access-list arp *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 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 \(968\)](#)

[show access-list arp \(969\)](#)

permit, deny (ARP ACL) This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

SYNTAX

```
[no] {permit | deny}  
    ip {any | host source-ip | source-ip ip-address-bitmask}  
    mac {any | host source-mac | source-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}  
    mac {any | host source-mac | source-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*²⁹ – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

*mac-address-bitmask*²⁹ – 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.

29. 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 \(967\)](#)

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: 16 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 \(968\)](#)

ACL INFORMATION

This section describes commands used to display ACL information.

Table 105: ACL Information Commands

Command	Function	Mode
clear access-list hardware counters	Clears hit counter for rules in all ACLs, or in a specified ACL.	PE
show access-group	Shows the ACLs assigned to each port	PE
show access-list	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 [*acl-name*]

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.³⁰

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.

30. Due to a hardware limitation, this option only displays statistics for permit rules.

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: 16 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#
```


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 106: Interface Commands

Command	Function	Mode
<i>Interface Configuration</i>		
interface	Configures an interface type and enters interface configuration mode	GC
alias	Configures an alias name for the interface	IC
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC
description	Adds a description to an interface configuration	IC
flowcontrol	Enables flow control on a given interface	IC
media-type	Force port type selected for combination ports	IC
negotiation	Enables autonegotiation of a given interface	IC
shutdown	Disables an interface	IC
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
switchport packet-rate*	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
clear counters	Clears statistics on an interface	PE
show interfaces brief	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
show interfaces counters	Displays statistics for the specified interfaces	NE, PE
show interfaces status	Displays status for the specified interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE
show interfaces transceiver	Displays the temperature, voltage, bias current, transmit power, and receive power	PE
<i>Cable Diagnostics</i>		
test cable-diagnostics	Performs cable diagnostics on the specified port	PE
show cable-diagnostics	Shows the results of a cable diagnostics test	PE

Table 106: Interface Commands (Continued)

Command	Function	Mode
<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

* Enabling hardware-level storm control with this command on a port will disable software-level automatic storm control on the same port if configured by the `auto-traffic-control` command (page 1029).

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: 1-28/52)

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

vlan *vlan-id* (Range: 1-4093)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

alias This command configures an alias name for the interface. Use the **no** form to remove the alias name.

SYNTAX

alias *string*

no alias

string - A mnemonic name 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 alias is displayed in the running-configuration file. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface.

EXAMPLE

The following example adds an alias to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#alias finance
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 | symmetric}

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

symmetric - When specified, the port transmits and receives symmetric pause frames.

DEFAULT SETTING

10GBASE-FX: 100full (SFP³¹ / SFP+)
1000BASE-T: 10half, 10full, 100half, 100full, 1000full
1000BASE-SX/LX/ZX (SFP³¹ / SFP+): 1000full
10GBASE-SR/LR/ER (SFP+): 10Gfull

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ 10GBASE-SFP+ connections are fixed at 10G, full duplex. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.
- ◆ 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 \(979\)](#)
[speed-duplex \(980\)](#)
[flowcontrol \(977\)](#)

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)

31. ECS4510-28F

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The description is displayed by the [show interfaces status](#) command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

EXAMPLE

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

flowcontrol This command enables flow control. Use the **no** form to disable flow control.

SYNTAX

[**no**] **flowcontrol**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- ◆ Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.
- ◆ To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- ◆ When using the [negotiation](#) command to enable auto-negotiation, the optimal settings will be determined by the [capabilities](#) command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port

EXAMPLE

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

RELATED COMMANDS

[negotiation \(979\)](#)

[capabilities \(flowcontrol, symmetric\) \(975\)](#)

media-type This command forces the port type selected for combination ports. Use the **no** form to restore the default mode.

SYNTAX

media-type *mode*

no media-type

mode

copper-forced - Always uses the built-in RJ-45 port.

sfp-forced - Always uses the SFP port (even if a module not installed).

sfp-preferred-auto - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

DEFAULT SETTING

Ports 23-24³²: sfp-preferred-auto

COMMAND MODE

Interface Configuration (Ethernet³²)

EXAMPLE

This forces the switch to use the built-in RJ-45 port for the combination port 24.

```
Console(config)#interface ethernet 1/24
Console(config-if)#media-type copper-forced
Console(config-if)#
```

32. ECS4510-28F

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 \(975\)](#)

[speed-duplex \(980\)](#)

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 \(979\)](#)

[capabilities \(975\)](#)

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 | unicast} packet-rate rate

no switchport {broadcast | multicast | unicast}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level in Kilobits per second.

(Range: 64-1,000,000 Kbps for 1G ports, 64-10,000,000 Kbps for 10G ports; Default: 64 Kbps)

DEFAULT SETTING

Broadcast Storm Control: Enabled, packet rate limit: 64 kbps

Multicast Storm Control: Disabled

Unknown Unicast Storm Control: Disabled

COMMAND MODE

Interface Configuration (Ethernet)

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.
- ◆ Traffic storms can be controlled at the hardware level using this command or at the software level using the [auto-traffic-control](#) command. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.
- ◆ The rate limits set by this command are also used by automatic storm control when the control response is set to rate limiting by the [auto-traffic-control action](#) command.

- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500," and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000" on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set by the storm control command. 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 Kilobits per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

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: 1-28/52)

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

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: 1-28/52)
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. For a description of the items displayed by this command, see ["Showing Port or Trunk Statistics" on page 162](#).

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
0 Error Output
0 Unknown Protocols Input
0 QLen Output
===== Extended Iftable Stats =====
23 Multi-cast Input
5525 Multi-cast Output
170 Broadcast Input
11 Broadcast Output
===== Ether-like Stats =====
0 Alignment Errors
0 FCS Errors
0 Single Collision Frames
0 Multiple Collision Frames
0 SQE Test Errors
0 Deferred Transmissions
0 Late Collisions
0 Excessive Collisions
0 Internal Mac Transmit Errors
0 Internal Mac Receive Errors
0 Frames Too Long
0 Carrier Sense Errors
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
21065 Packet Size <= 64 Octets
3805 Packet Size 65 to 127 Octets
2448 Packet Size 128 to 255 Octets
797 Packet Size 256 to 511 Octets
2941 Packet Size 512 to 1023 Octets
9187 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#
```

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: 1-28/52)
        port-channel channel-id (Range: 1-16)
        vlan vlan-id (Range: 1-4093)
```

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. For a description of the items displayed by this command, see ["Displaying Connection Status" on page 155](#).

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
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 64 Kbits/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 64 Kbits/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control        : Disabled
  VLAN Trunking       : Disabled
  LACP                : Disabled
  Media Type          : None
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: 1-28/52)
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
GVRP Status                   : Disabled
Allowed VLAN                   : 1(u)
Forbidden VLAN                 :
802.1Q Tunnel Status          : Disabled
802.1Q Tunnel Mode            : Normal
802.1Q Tunnel TPID            : 8100 (Hex)
Layer 2 Protocol Tunnel       : None
Console#
```

Table 107: show interfaces switchport - display description

Field	Description
Broadcast Threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 981).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 981).

Table 107: 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 981).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 996).
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 1131).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 1130).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 1128).
Native VLAN	Indicates the default Port VLAN ID (page 1131).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 1170).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 1122).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 1129).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 1122).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 1136).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 1137).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 1140).
Layer 2 Protocol Tunnel	Shows if L2 Protocol Tunnel is enabled for spanning tree protocol (page 1144).

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: SFP ports 25-28)

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.

EXAMPLE

```
Console#show interfaces transceiver ethernet 1/25
Information of Eth 1/25
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
Console#
```

Cable Diagnostics

test cable-diagnostics This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

SYNTAX

test cable-diagnostics interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

COMMAND MODE

Privileged Exec

COMMAND USAGE

- ◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test methods. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- ◆ This cable test is only accurate for cables 7 - 140 meters long.

- ◆ 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.
- ◆ 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.

EXAMPLE

```
Console#test cable-diagnostics interface ethernet 1/24
Console#
```

show cable-diagnostics This command shows the results of a cable diagnostics test.

SYNTAX

show cable-diagnostics interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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 include:
 - OK: Correctly terminated pair
 - Open: Open pair, no link partner
 - Short: Shorted pair
 - Not Supported: This message is displayed for any Fast Ethernet ports that are linked up, or for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
 - Impedance mismatch: Terminating impedance is not in the reference range.

EXAMPLE

```
Console#show cable-diagnostics interface ethernet 1/24
Port      Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-----
Eth 1/24 GE   Up      OK (1)          OK (1)          2012-08-09 10:24:49
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)

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 (enters 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 mode on a active link only works when the connection speed is 100 Mbps or higher at linkup, and line length is less than 60 meters.

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: 1-24/48)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show power-save interface ethernet 1/24
Power Saving Status:
 Ethernet 1/24 : Enabled
Console#
```


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 108: 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 : 64 Kbits/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 64 Kbits/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control        : Disabled
  VLAN Trunking       : Disabled
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.

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.

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** | **sys-id**}

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.

sys-id - 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
-----
Eth 1/ 2
-----
LACPDU Sent      : 12
LACPDU Received  : 6
Marker Sent      : 0
Marker Received  : 0
```

```
LACPDUs Unknown Pkts : 0
LACPDUs Illegal Pkts : 0
:
```

Table 109: show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	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.
LACPDUs Illegal Pkts	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
-----
Oper Key   : 3
Admin Key  : 0
Timeout    : long

Eth 1/ 1
-----
LACPDUs Internal      : 30 seconds
LACP System Priority  : 32768
LACP Port Priority    : 32768
Admin Key             : 3
Oper Key              : 3
Admin State           : defaulted, aggregation, long timeout, LACP-activity
Oper State            : distributing, collecting, synchronization,
                       aggregation, long timeout, LACP-activity
:
```

Table 110: show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
Timeout	Time to wait for the next LACPDU before deleting partner port information.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.

Table 110: show lacp internal - display description (Continued)

Field	Description
Admin State, Oper State	<p>Administrative or operational values of the actor's state parameters:</p> <ul style="list-style-type: none"> Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```

Console#show lacp 1 neighbors
Port Channel 1 neighbors
-----
Eth 1/ 1
-----
Partner Admin System ID   : 32768, 00-00-00-00-00-00
Partner Oper System ID   : 32768, 00-12-CF-61-24-2F
Partner Admin Port Number : 1
Partner Oper Port Number  : 1
Port Admin Priority        : 32768
Port Oper Priority         : 32768
Admin Key                  : 0
Oper Key                   : 3
Admin State:               defaulted, distributing, collecting,
                           synchronization, long timeout,
Oper State:               distributing, collecting, synchronization,
                           aggregation, long timeout, LACP-activity
:

```

Table 111: show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.

Table 111: show lacp neighbors - display description (Continued)

Field	Description
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```

Console#show lacp sysid
Port Channel      System Priority    System MAC Address
-----
                1          32768      00-30-F1-8F-2C-A7
                2          32768      00-30-F1-8F-2C-A7
                3          32768      00-30-F1-8F-2C-A7
                4          32768      00-30-F1-8F-2C-A7
                5          32768      00-30-F1-8F-2C-A7
                6          32768      00-30-F1-8F-2C-A7
                7          32768      00-30-F1-D4-73-A0
                8          32768      00-30-F1-D4-73-A0
                9          32768      00-30-F1-D4-73-A0
               10          32768      00-30-F1-D4-73-A0
               11          32768      00-30-F1-D4-73-A0
               12          32768      00-30-F1-D4-73-A0
               :

```

Table 112: 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#

```


The commands in this group control the power that can be delivered to attached PoE devices through the RJ-45 ports 1-24/48 on the ECS4510-28P/52P.

The switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Table 113: PoE Commands

Command	Function	Mode
<code>power inline</code>	Turns power on and off for specific ports	IC
<code>power inline maximum allocation</code>	Sets the maximum power available to specific switch ports	IC
<code>power inline priority</code>	Sets the priority for power supplied to specific ports	IC
<code>show power inline status</code>	Displays the current status of power management on specific ports or all ports	PE
<code>show power mainpower</code>	Displays the current status of power management for switch	PE

power inline This command instructs the switch to automatically detect if a PoE-compliant device is connected to the specified port, and turn power on or off accordingly. Use the **no** form to turn off power for a port.

SYNTAX

[no] power inline

DEFAULT SETTING

Detection is enabled for PoE-compliant devices.

COMMAND MODE

Interface Configuration (ECS4510-28P/52P Ethernet ports 1-24/48)

COMMAND USAGE

- ◆ The switch only provides power to the Gigabit Ethernet RJ-45 ports.

- ◆ When detection is enabled for PoE-compliant devices, power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed the port's power budget or the switch's power budget.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#no power inline
Console(config-if)#
```

power inline maximum allocation

This command limits the power allocated to specific ports. Use the **no** form to restore the default setting.

SYNTAX

power inline maximum allocation *milliwatts*
no power inline maximum allocation

milliwatts - The maximum power budget for the port.
 (Range: 3000 - 30000 milliwatts)

DEFAULT SETTING

30000 milliwatts

COMMAND MODE

Interface Configuration (ECS4510-28P/52P Ethernet ports 1-24/48)

COMMAND USAGE

- ◆ The ECS4510-28P can supply up to 30W of power for 13 ports (based on IEEE 802.3at), or up to 15.4W to 24 ports (based on IEEE 802.3af).
- ◆ The ECS4510-52P can supply up to 30W of power for 25 ports (based on IEEE 802.3at), or up to 15.4W to 48 ports (based on IEEE 802.3af).
- ◆ If a device is connected to a switch port and the switch detects that it requires more than the maximum power allocated to the port or to the overall switch, no power is supplied to the device (i.e., port power remains off).

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline maximum allocation 8000
Console(config-if)#
```

power inline priority This command sets the power priority for specific ports. Use the **no** form to restore the default setting.

SYNTAX

power inline priority *priority*
no power inline priority

priority - The power priority for the port.
 Options: 1 (critical), 2 (high), or 3 (low)

DEFAULT SETTING

3 (low)

COMMAND MODE

Interface Configuration

COMMAND USAGE

- ◆ If the power demand from devices connected to the switch exceeds the power budget setting as determined during bootup, the switch uses port power priority settings to control the supplied power. For example:
 - A device connected to a low-priority port that causes the switch to exceed its budget is not supplied power.
 - If a device is connected to a critical or high-priority port and causes the switch to exceed its budget, port power is still be turned on if the switch can drop power to one or more lower-priority ports and keep within its budget.

 Power will be dropped from lower-priority ports starting in reverse sequence from ECS4510-28P/52P port number 24/48.
 - If sufficient power cannot be freed up for a critical or high-priority port by turning off power to lower-priority ports, power will not be supplied to the newly connected device.
- ◆ If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port regardless of its priority setting.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline priority 2
Console(config-if)#
```

show power inline status This command displays the current power status for all ports or for specific ports.

SYNTAX

show power inline status [*interface*]

interface

ethernet

unit - Unit identifier. (Range: 1)

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

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show power inline status
Unit: 1
Compatible mode : Enabled

```

Interface	Admin	Oper	Max Power	Used Power	Priority
Eth 1/ 1	Enabled	Off	30000 mW	0 mW	Low
Eth 1/ 2	Enabled	Off	30000 mW	0 mW	Low
Eth 1/ 3	Enabled	Off	30000 mW	7505 mW	Low
Eth 1/ 4	Enabled	Off	30000 mW	0 mW	Low
Eth 1/ 5	Enabled	Off	30000 mW	0 mW	Low
Eth 1/ 6	Enabled	Off	30000 mW	0 mW	Low
Eth 1/ 7	Enabled	Off	15400 mW	8597 mW	Low
Eth 1/ 8	Enabled	Off	15400 mW	0 mW	Low
Eth 1/ 9	Enabled	Off	15400 mW	0 mW	Low
Eth 1/10	Enabled	Off	15400 mW	0 mW	Low
Eth 1/11	Enabled	Off	15400 mW	0 mW	Low
Eth 1/12	Enabled	Off	15400 mW	0 mW	Low
:					

Table 114: **show power inline status** - display description

Field	Description
Admin	The power mode set on the port (see power inline)
Oper	The current operating power status (displays on or off)
Power (mWatt)	The maximum power allocated to this port (see power inline maximum allocation)
Power (used)	The current power consumption on the port in milliwatts
Priority	The port's power priority setting (see power inline priority)

show power mainpower Use this command to display the current power status for the switch.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show power mainpower
Unit 1 Main Power Status
  PoE Maximum Available Power : 410 Watts
  System Operation Status      : On
  PoE Power Consumption        : 0 Watts
  Software Version             : Version 0148 (Hex), Build 66 (Hex)
Console#
```

Table 115: **show power mainpower** - display description

Field	Description
PoE Maximum Available Power	The available power budget for the switch
System Operation Status	The current operating power status (displays on or off)
PoE Power Consumption	The current power consumption on the switch in watts
Software Version	The version of software running on the PoE controller subsystem in the switch.

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 116: 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 117: Mirror Port Commands

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

port monitor This command configures a mirror session. Use the **no** form to clear a mirror session.

SYNTAX

port monitor {*interface* [**rx** | **tx** | **both**] | **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: 1-28/52)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

vlan-id - VLAN ID (Range: 1-4093)

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

acl-name - Name of the ACL. (Maximum length: 16 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.
- ◆ All VLAN mirror sessions must share the same target port, preferably one that is not a member of the source VLAN.
- ◆ 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.
- ◆ Note that 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 ([page 949](#)) 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*]

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

unit - Unit identifier. (Range: 1)

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

vlan-id - VLAN ID (Range: 1-4093)

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

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):Eth1/5
Source Port (monitored port)  :Eth1/6
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 118: 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.

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled, then no session can be configured for RSPAN.

- ◆ *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)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the [port monitor](#) command, then there is only one session available for RSPAN.

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: 1-28/52)

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.
- ◆ 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)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the [port monitor](#) command, then there is only one session available for RSPAN.

interface - **ethernet** *unit/port*

unit - Unit identifier. (Range: 1)

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

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)

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled with the [port monitor](#) command, then no session can be configured for RSPAN.

vlan-id - ID of configured RSPAN VLAN. (Range: 2-4092)
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: 1-28/52)

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)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the `port monitor` command, then there is only one session available for RSPAN.

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)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the [port monitor](#) command, then there is only one session available for RSPAN.

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#
```

This function allows 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 119: Rate Limit Commands

Command	Function	Mode
<code>rate-limit</code>	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 restore the default rate. Use the **no** form to restore the default status of disabled.

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. For example, suppose broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500," and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000" on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set

by the storm control command. 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 \(986\)](#)

AUTOMATIC TRAFFIC CONTROL COMMANDS

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Table 120: ATC Commands

Command	Function	Mode
<i>Threshold Commands</i>		
<code>auto-traffic-control apply-timer</code>	Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold	GC
<code>auto-traffic-control release-timer</code>	Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold	GC
<code>auto-traffic-control*</code>	Enables automatic traffic control for broadcast or multicast storms	IC (Port)
<code>auto-traffic-control action</code>	Sets the control action to limit ingress traffic or shut down the offending port	IC (Port)
<code>auto-traffic-control alarm-clear-threshold</code>	Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent	IC (Port)
<code>auto-traffic-control alarm-fire-threshold</code>	Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires	IC (Port)
<code>auto-traffic-control auto-control-release</code>	Automatically releases a control response	IC (Port)
<code>auto-traffic-control control-release</code>	Manually releases a control response	IC (Port)
<i>SNMP 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)

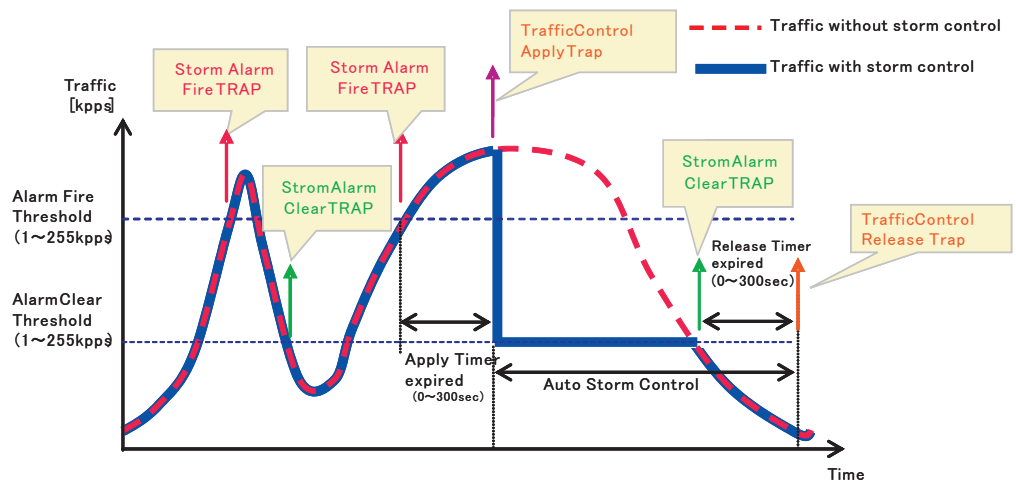
Table 120: ATC Commands (Continued)

Command	Function	Mode
<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>ATC Display Commands</i>		
<code>show auto-traffic-control</code>	Shows global configuration settings for automatic storm control	PE
<code>show auto-traffic-control interface</code>	Shows interface configuration settings and storm control status for the specified port	PE

* Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the `switchport packet-rate` command.

USAGE GUIDELINES

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Figure 427: Storm Control by Limiting the Traffic Rate

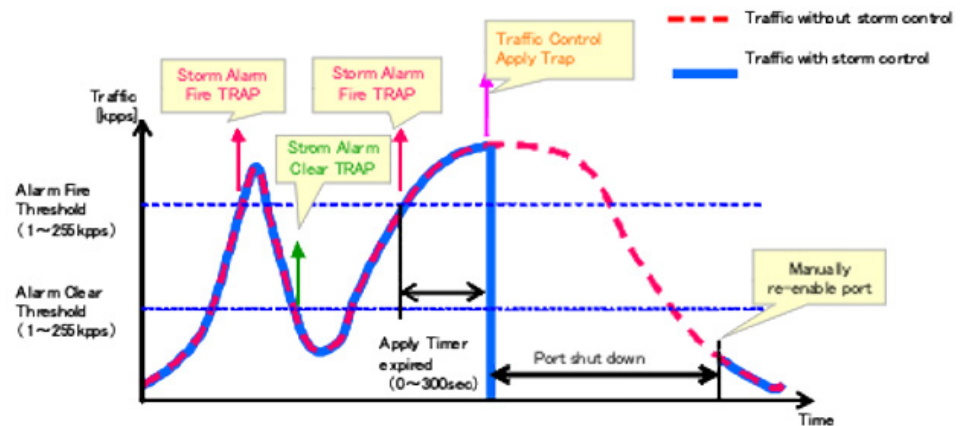
The key elements of this diagram are described below:

- ◆ **Alarm Fire Threshold** – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- ◆ When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- ◆ **Alarm Clear Threshold** – The lower threshold beneath which a control response can be automatically terminated after the release timer

expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.

- ◆ When traffic falls below the alarm clear threshold after the release timer expires, traffic control (for rate limiting) will be stopped and a Traffic Control Release Trap sent and logged. Note that if the control action has shut down a port, it can only be manually re-enabled using the [auto-traffic-control control-release](#) command).
- ◆ The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Figure 428: Storm Control by Shutting Down a Port



The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

FUNCTIONAL LIMITATIONS

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the [switchport packet-rate](#) command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

Threshold Commands

auto-traffic-control apply-timer

This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {broadcast | multicast} apply-timer *seconds*

no auto-traffic-control {broadcast | multicast} apply-timer

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 1-300 seconds)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

After the apply timer expires, a control action may be triggered as specified by the [auto-traffic-control action](#) command and a trap message sent as specified by the [snmp-server enable port-traps atc broadcast-control-apply](#) command or [snmp-server enable port-traps atc multicast-control-apply](#) command.

EXAMPLE

This example sets the apply timer to 200 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the **no** form to restore the default setting.

SYNTAX

**auto-traffic-control {broadcast | multicast}
release-timer *seconds***

no auto-traffic-control {broadcast | multicast} release-timer

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold.
(Range: 1-900 seconds)

DEFAULT SETTING

900 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the delay after which the control response can be terminated. The [auto-traffic-control auto-control-release](#) command must be used to enable or disable the automatic release of a control response of rate-limiting. To re-enable a port which has been shut down by automatic traffic control, you must manually re-enable the port using the [auto-traffic-control control-release](#) command.

EXAMPLE

This example sets the release timer to 800 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

auto-traffic-control This command enables automatic traffic control for broadcast or multicast storms. Use the **no** form to disable this feature.

SYNTAX

[no] auto-traffic-control {broadcast | multicast}

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- ◆ Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.
- ◆ Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the [switchport packet-rate](#) command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

EXAMPLE

This example enables automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control action

This command sets the control action to limit ingress traffic or shut down the offending port. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
action {**rate-control** | **shutdown**}

no auto-traffic-control {**broadcast** | **multicast**} **action**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

rate-control - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the [auto-traffic-control alarm-clear-threshold](#) command.

shutdown - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

DEFAULT SETTING

rate-control

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- ◆ When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.
- ◆ When the control response is set to rate limiting by this command, the rate limits are determined by the [auto-traffic-control alarm-clear-threshold](#) command.
- ◆ If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.
- ◆ If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the [auto-traffic-control control-release](#) command.

EXAMPLE

This example sets the control response for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

**auto-traffic-control
alarm-clear-
threshold**

This command sets the lower threshold for ingress traffic beneath which a control response for rate limiting will be released after the Release Timer expires, if so configured by the [auto-traffic-control auto-control-release](#) command. Use the **no** form to restore the default setting.

SYNTAX

**auto-traffic-control {broadcast | multicast}
alarm-clear-threshold *threshold***

**no auto-traffic-control {broadcast | multicast}
alarm-clear-threshold**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second)

DEFAULT SETTING

128 kilo-packets per second

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- ◆ Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the [snmp-server enable port-traps atc broadcast-alarm-clear](#) command or [snmp-server enable port-traps atc multicast-alarm-clear](#) command.
- ◆ If rate limiting has been configured as a control response, it will be discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the [auto-traffic-control control-release](#) command.

EXAMPLE

This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

SYNTAX

**auto-traffic-control {broadcast | multicast}
alarm-fire-threshold *threshold***

**no auto-traffic-control {broadcast | multicast}
alarm-fire-threshold**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires.
(Range: 1-255 kilo-packets per second)

DEFAULT SETTING

128 kilo-packets per second

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- ◆ Once the upper threshold is exceeded, a trap message may be sent if configured by the [snmp-server enable port-traps atc broadcast-alarm-fire](#) command or [snmp-server enable port-traps atc multicast-alarm-fire](#) command.
- ◆ After the upper threshold is exceeded, the control timer must first expire as configured by the [auto-traffic-control apply-timer](#) command before a control response is triggered if configured by the [auto-traffic-control action](#) command.

EXAMPLE

This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

auto-traffic-control auto-control-release This command automatically releases a control response of rate-limiting after the time specified in the [auto-traffic-control release-timer](#) command has expired.

SYNTAX

**auto-traffic-control {broadcast | multicast}
auto-control-release**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- ◆ This command can be used to automatically stop a control response of rate-limiting after the specified action has been triggered and the release timer has expired.
- ◆ To release a control response which has shut down a port after the specified action has been triggered and the release timer has expired, use the [auto-traffic-control control-release](#) command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

auto-traffic-control control-release This command manually releases a control response.

SYNTAX

auto-traffic-control {broadcast | multicast} control-release

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command can be used to manually stop a control response of rate-limiting or port shutdown any time after the specified action has been triggered.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast control-release
Console(config-if)#
```

SNMP Trap Commands

snmp-server enable port-traps atc broadcast-alarm- clear

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[no] snmp-server enable port-traps atc broadcast-alarm-clear

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control action \(1030\)](#)

[auto-traffic-control alarm-clear-threshold \(1031\)](#)

snmp-server enable port-traps atc broadcast-alarm-fire

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[no] snmp-server enable port-traps atc broadcast-alarm-fire

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control alarm-fire-threshold \(1032\)](#)**snmp-server enable
port-traps atc
broadcast-control-
apply**

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[no] snmp-server enable port-traps atc broadcast-control-apply

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control alarm-fire-threshold \(1032\)](#)[auto-traffic-control apply-timer \(1028\)](#)**snmp-server enable
port-traps atc
broadcast-control-
release**

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

**[no] snmp-server enable port-traps atc
broadcast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-
release
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control alarm-clear-threshold \(1031\)](#)
[auto-traffic-control action \(1030\)](#)
[auto-traffic-control release-timer \(1028\)](#)

snmp-server enable port-traps atc multicast-alarm- clear

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[no] snmp-server enable port-traps atc multicast-alarm-clear

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control action \(1030\)](#)
[auto-traffic-control alarm-clear-threshold \(1031\)](#)

snmp-server enable port-traps atc multicast-alarm-fire

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[no] snmp-server enable port-traps atc multicast-alarm-fire

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```


RELATED COMMANDS

[auto-traffic-control alarm-fire-threshold \(1032\)](#)

snmp-server enable port-traps atc multicast-control- apply

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[no] snmp-server enable port-traps atc multicast-control-apply

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-apply
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control alarm-fire-threshold \(1032\)](#)

[auto-traffic-control apply-timer \(1028\)](#)

snmp-server enable port-traps atc multicast-control- release

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

**[no] snmp-server enable port-traps atc
multicast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-
release
Console(config-if)#
```

RELATED COMMANDS

[auto-traffic-control alarm-clear-threshold \(1031\)](#)
[auto-traffic-control action \(1030\)](#)
[auto-traffic-control release-timer \(1028\)](#)

ATC Display Commands

show auto-traffic-control This command shows global configuration settings for automatic storm control.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show auto-traffic-control

Storm Control Broadcast
  Apply Timer (sec)    : 300
  Release Timer (sec)  : 900

Storm Control Multicast
  Apply Timer (sec)    : 300
  Release Timer (sec)  : 900
Console#
```

show auto-traffic-control interface This command shows interface configuration settings and storm control status for the specified port.

SYNTAX

show auto-traffic-control interface [*interface*]
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
-----
Storm Control:          Broadcast          Multicast
State:                  Disabled           Disabled
Action:                 Rate Control       Rate Control
Auto Release Control:   Disabled           Disabled
Alarm Fire Threshold(Kpps): 128             128
Alarm Clear Threshold(Kpps):128             128
Trap Storm Fire:        Disabled           Disabled
```

Trap Storm Clear:	Disabled	Disabled
Trap Traffic Apply:	Disabled	Disabled
Trap Traffic Release:	Disabled	Disabled

Console#

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 121: 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 mode</code>	Specifies shutdown by dropping packets for ports detected in loopback state or by dropping packets belonging to VLANs detected in loopback state	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 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 command described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.
- ◆ When a loopback event is detected on an interface or when a interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- ◆ Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

loopback-detection This command enables loopback detection globally on the switch or on a specified interface. Use the **no** form to disable loopback detection.

SYNTAX

[no] loopback-detection

DEFAULT SETTING

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 mode This command specifies shutdown by dropping packets for a port detected in loopback state or by dropping packets belonging to a VLAN detected in loopback state. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection mode {port-based | vlan-based}

no loopback-detection mode

port-based - When loopback is detected on a port, the port is shut down automatically.

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

DEFAULT SETTING

port-based

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ When using vlan-based mode, loopback detection control frames are untagged or tagged depending on the port's VLAN membership type.
- ◆ When using vlan-based mode, 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 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.

EXAMPLE

This example sets the loopback detection mode to VLAN based.

```
Console(config)#loopback-detection mode vlan-based
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 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: 1-28/52)

COMMAND MODE
Privileged Exec**EXAMPLE**

```
Console#show loopback-detection
Loopback Detection Global Information
Global Status      : Enabled
Transmit Interval  : 10
Recover Time       : 60
Mode               : Port-based
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
Console#
```


UniDirectional Link Detection Commands

The switch can be configured to detect and disable unidirectional Ethernet fiber or copper links. When enabled, the protocol advertises a port's identity and learns about its neighbors on a specific LAN segment; and stores information about its neighbors in a cache. It can also send out a train of echo messages under circumstances that require fast notifications or resynchronization of the cached information.

Table 122: UniDirectional Link Detection Commands

Command	Function	Mode
<code>udld message-interval</code>	Configures the message interval between UDLD probe messages	GC
<code>udld aggressive</code>	Sets UDLD to aggressive mode on an interface	IC
<code>udld port</code>	Enables UDLD on an interface	IC
<code>show udld</code>	Shows UDLD configuration settings and operational status	PE

udld message-interval This command configures the message interval between UDLD probe messages for ports in advertisement phase and determined to be bidirectional. Use the **no** form to restore the default setting.

SYNTAX

udld message-interval *message-interval*

no message-interval

message-interval – The interval at which a port sends UDLD probe messages after linkup or detection phases. (Range: 7-90 seconds)

DEFAULT SETTING

15 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171.

If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds).

If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.

EXAMPLE

This example sets the message interval to 10 seconds.

```
Console(config)#udld message-interval 10
Console(config)#
```

udld aggressive This command sets UDLD to aggressive mode on an interface. Use the **no** form to restore the default setting.

SYNTAX

[no] udld aggressive

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet Port)

COMMAND USAGE

UDLD can function in two modes: normal mode and aggressive mode.

- ◆ In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that's information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are "event-based." If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach minimize false positives during the detection process and deems a port to be in "undetermined" state. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.
- ◆ In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity

problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is optional and is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).

EXAMPLE

This example enables UDLD aggressive mode on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#udld aggressive
Console(config-if)#
```

udld port This command enables UDLD on an interface. Use the **no** form to disable UDLD on an interface.

SYNTAX

[no] udld port

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet Port)

COMMAND USAGE

- ◆ UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential misconfiguration to be detected and for prompt corrective action to be taken.
- ◆ Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.)

Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is considered to be unidirectional.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#udld port
Console(config-if)#
```

show udld This command shows UDLD configuration settings and operational status for the switch or for a specified interface.

SYNTAX

```
show udld [interface interface]
           interface
           ethernet unit/port
           unit - Unit identifier. (Range: 1)
           port - Port number. (Range: 1-28/52)
```

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show udld
Message Interval : 15

Interface UDLD      Mode      Oper State      Msg Invl
                  Port State      Timeout
-----
Eth 1/ 1  Enabled  Aggressive  Advertisement    15 s
                  Bidirectional    5 s
Eth 1/ 2  Disabled Normal      Disabled         7 s
                  Unknown         5 s
Eth 1/ 3  Disabled Normal      Disabled         7 s
                  Unknown         5 s
Eth 1/ 4  Disabled Normal      Disabled         7 s
                  Unknown         5 s
Eth 1/ 5  Disabled Normal      Disabled         7 s
                  Unknown         5 s
:
Console#show udld interface ethernet 1/1
Interface UDLD      Mode      Oper State      Msg Invl
                  Port State      Timeout
-----
Eth 1/ 1  Enabled  Aggressive  Advertisement    15 s
                  Bidirectional    5 s
Console#
```

Table 123: show udld - display description

Field	Description
Message Interval	The interval between UDLD probe messages for ports in advertisement phase
UDLD	Shows if UDLD is enabled or disabled on a port
Mode	Shows if UDLD is functioning in Normal or Aggressive mode
Oper State	Shows the UDLD operational state (Disabled, Link down, Link up, Advertisement, Detection, Disabled port, Advertisement - Single neighbor, Advertisement - Multiple neighbors)

Table 123: show udld - display description (Continued)

Field	Description
Port State	Shows the UDLD port state (Unknown, Bidirectional, Unidirectional, Transmit-to-receive loop, Mismatch with neighbor state reported, Neighbor's echo is empty) The state is Unknown if the link is down or not connected to a UDLD-capable device. The state is Bidirectional if the link has a normal two-way connection to a UDLD-capable device. All other states indicate miswiring.
Msg Invl	The interval between UDLD probe messages used for the indicated operational state
Timeout	The time that UDLD waits for echoes from a neighbor device during the detection window

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 124: Address Table Commands

Command	Function	Mode
<code>mac-address-table aging-time</code>	Sets the aging time of the address table	GC
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>clear mac-address-table dynamic</code>	Removes any learned entries from the forwarding database	PE
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show mac-address-table aging-time</code>	Shows the aging time for the address table	PE
<code>show mac-address-table count</code>	Shows the number of MAC addresses used and the number of available MAC addresses	PE

mac-address-table aging-time This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

SYNTAX

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 6-672 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: 1-28/52)

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

vlan-id - VLAN ID (Range: 1-4093)

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

DEFAULT SETTING

No static addresses are defined. The default mode is **permanent**.

COMMAND MODE

Global Configuration

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- ◆ Static addresses will not be removed from the address table when a given interface link is down.
- ◆ Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- ◆ A static address cannot be learned on another port until the address is removed with the **no** form of this command.

EXAMPLE

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear mac-address-table dynamic
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: 1-28/52)

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

vlan-id - VLAN ID (Range: 1-4093)

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
- ◆ 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: 1-28/52)
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 Port ID   :1
Dynamic Address Count     :2
Total MAC Addresses       :2
Total MAC Address Space Available: 16384
Console#
```


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 125: 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 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 mst configuration</code>	Changes to MSTP configuration mode	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
<code>spanning-tree loopback-detection action</code>	Configures the response for loopback detection to block user traffic or shut down the interface	IC

Table 125: Spanning Tree Commands (Continued)

Command	Function	Mode
<code>spanning-tree loopback-detection release-mode</code>	Configures loopback release mode for a port	IC
<code>spanning-tree loopback-detection trap</code>	Enables BPDU loopback SNMP trap notification for a port	IC
<code>spanning-tree mst cost</code>	Configures the path cost of an instance in the MST	IC
<code>spanning-tree mst port-priority</code>	Configures the priority of an instance in the MST	IC
<code>spanning-tree port-bpdu-flooding</code>	Floods BPDUs to other ports when global spanning tree is disabled	IC
<code>spanning-tree port-priority</code>	Configures the spanning tree priority of an interface	IC
<code>spanning-tree root-guard</code>	Prevents a designated port from passing superior BPDUs	IC
<code>spanning-tree spanning-disabled</code>	Disables spanning tree for an interface	IC
<code>spanning-tree loopback-detection release</code>	Manually releases a port placed in discarding state by loopback-detection	PE
<code>spanning-tree protocol-migration</code>	Re-checks the appropriate BPDU format	PE
<code>show spanning-tree</code>	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
<code>show spanning-tree mst configuration</code>	Shows the multiple spanning tree configuration	PE

spanning-tree This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

SYNTAX

[no] spanning-tree

DEFAULT SETTING

Spanning tree is enabled.

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.

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 \(1061\)](#)

[spanning-tree max-age \(1063\)](#)

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 \(1061\)](#)

[spanning-tree hello-time \(1062\)](#)

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 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 1073](#)) takes precedence over port priority ([page 1080](#)).
- ◆ 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 40000
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 \(1069\)](#)
[mst priority \(1068\)](#)
[name \(1070\)](#)
[revision \(1070\)](#)
[max-hops \(1068\)](#)

**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
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: 1-4093)

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 32 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 1070](#)) 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 the spanning tree.

DEFAULT SETTING

Switch's MAC address

COMMAND MODE

MST Configuration

COMMAND USAGE

The MST region name and revision number ([page 1070](#)) 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 \(1070\)](#)

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 1070](#)) 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 \(1070\)](#)

spanning-tree bpd
filter This command filters all BPDUs received on an edge port. 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 filters all Bridge Protocol Data Units (BPDUs) received on an interface 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.
- ◆ Before enabling BPDU Filter, the interface must first be configured as an edge port with the [spanning-tree edge-port](#) command.

EXAMPLE

```

Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#

```

RELATED COMMANDS

[spanning-tree edge-port \(1074\)](#)

spanning-tree bpdu-guard This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form without any keywords to disable this feature, or with a keyword to restore the default settings.

SYNTAX

spanning-tree bpdu-guard [**auto-recovery** [**interval** *interval*]]

no spanning-tree bpdu-guard [**auto-recovery** [**interval**]]

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

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.
- ◆ Before enabling BPDU Guard, the interface must be configured as an edge port with the [spanning-tree edge-port](#) command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

EXAMPLE

```

Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#

```

RELATED COMMANDS[spanning-tree edge-port \(1074\)](#)[spanning-tree spanning-disabled \(1082\)](#)

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 method³³, 1-200,000,000 for long path cost method)

Table 126: Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (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 127: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (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)

33. Use the [spanning-tree pathcost method](#) command on [page 1065](#) to set the path cost method.

COMMAND USAGE

- ◆ This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- ◆ Path cost takes precedence over port priority.
- ◆ When the path cost method ([page 1065](#)) 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.

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 block user traffic or 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

block - Blocks user traffic.

shutdown - Shuts down the interface.

duration - The duration to shut down the interface.
(Range: 60-86400 seconds)

DEFAULT SETTING

block

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
```


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 BPDUs. Use the **no** form to restore the default.

SYNTAX

[no] spanning-tree loopback-detection trap

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

SYNTAX

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

instance-id - Instance identifier of the spanning tree.
(Range: 0-4094)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method³⁴, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in [Table 126 on page 1073](#).

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 127 on page 1073](#).

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ Each spanning-tree instance is associated with a unique set of VLAN IDs.

³⁴. Use the [spanning-tree pathcost method](#) command to set the path cost method.

- ◆ 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 \(1079\)](#)

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 \(1078\)](#)**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.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

RELATED COMMANDS

[spanning-tree cost \(1073\)](#)

spanning-tree root-guard

This command prevents a designated port³⁵ 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.

35. See Port Role under ["Displaying Interface Settings for STA" on page 250](#).

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)

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
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: 1-28/52)
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: 1-28/52)

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 eth 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: 1-28/52)

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.
- ◆ For a description of the items displayed under "Spanning-tree information," see ["Configuring Global Settings for STA" on page 240](#). For a description of the items displayed for specific interfaces, see ["Displaying Interface Settings for STA" on page 250](#).

EXAMPLE

```

Console#show spanning-tree
Spanning Tree Information
-----
Spanning Tree Mode           : MSTP
Spanning Tree Enabled/Disabled : Enabled
Instance                     : 0
VLANs Configured             : 1-4093
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
.
.
.

```

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          Edge
-----
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      1-4093
Console#

```

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 128: 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
<code>clear erps statistics</code>	Clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages	PE

Table 128: ERPS Commands(Continued)

Command	Function	Mode
<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 \(1091\)](#)

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

[no] erps domain *ring-name* [**id** *ring-id*]

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: 1-4093)

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 1126](#)), add the ring ports for the east and west interface as tagged members to this VLAN ([switchport allowed vlan](#), [page 1129](#)), 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 \(1089\)](#)

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 \(1301\)](#)
[ethernet cfm mep \(1306\)](#)

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" on page 485](#).

EXAMPLE

```
Console(config-erps)#mep-monitor east mep 1
Console(config-erps)#
```

RELATED COMMANDS[ethernet cfm domain \(1301\)](#)[ethernet cfm mep \(1306\)](#)

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

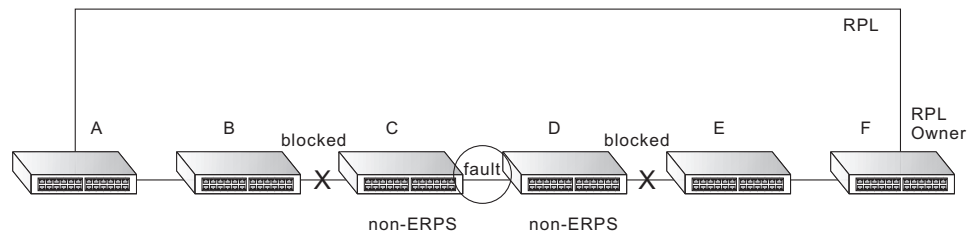
COMMAND MODE

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 1295](#). 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.



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.

- 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 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)#propagate-tc
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

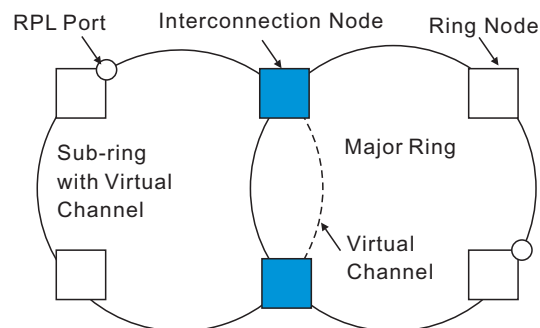
ERPS Configuration

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.

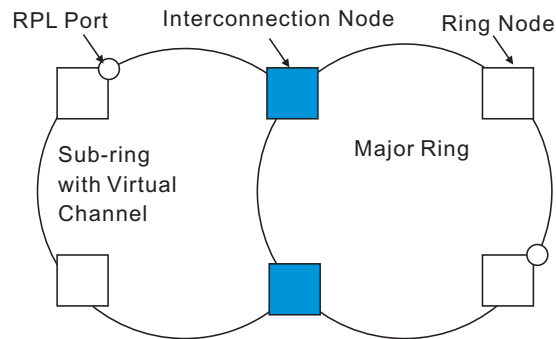
Figure 429: Sub-ring with Virtual Channel



- ◆ 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 430: 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: 1-28/52)

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 129 on page 1110](#)). 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 129: ERPS Request/State Priority

Request / State and Status	Type	Priority
Clear	local	highest
FS	local	

Table 129: ERPS Request/State Priority (Continued)

Request / State and Status	Type	Priority
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 129 on page 1110](#)). 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	1	Blocking	No		No		No			Yes
East	Eth 1/ 3	3	Forwarding	No		No		No			No

```
Console#
```

Table 130: **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.
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 130 on page 1114 describes most of the parameters shown by **show erps domain** command. The following table includes the remaining parameters.

Table 131: **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.
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.

Table 131: **show erps domain** - detailed display description (Continued)

Field	Description
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 132: **show erps statistics** - detailed display description

Field	Description
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

Table 132: **show erps statistics** - detailed display description (Continued)

Field	Description
EVENT	Any request/state message, excluding FS, SF, MS, and NR
HEALTH	The number of non-standard health-check messages

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 133: VLAN Commands

Command Group	Function
GVRP and Bridge Extension Commands	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring IEEE 802.1Q Tunneling	Configures 802.1Q Tunneling (QinQ Tunneling)
Configuring L2CP Tunneling*	Configures Layer 2 Control Protocol (L2CP) tunneling, either by discarding, processing, or transparently passing control packets across a QinQ tunnel
Configuring VLAN Translation*	Maps VLAN ID between customer and service provider for networks that do not support IEEE 802.1Q tunneling
Configuring Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports
Configuring Protocol-based VLANs	Configures protocol-based VLANs based on frame type and protocol
Configuring IP Subnet VLANs	Configures IP Subnet-based VLANs
Configuring MAC Based VLANs	Configures MAC-based VLANs
Configuring Voice VLANs	Configures VoIP traffic detection and enables a Voice VLAN

* These functions are not compatible.

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 134: 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 are applied to GVRP for all the ports on all VLANs.
- ◆ Timer values must meet the following restrictions:
 - leave \geq (3 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 \(1124\)](#)

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: 1-4093).

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.
- ◆ 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).

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

COMMAND USAGE

See ["Displaying Bridge Extension Capabilities"](#) on page 123 for a description of the displayed items.

EXAMPLE

```
Console#show bridge-ext
Maximum Supported VLAN Numbers      : 4093
Maximum Supported VLAN ID           : 4093
Extended Multicast Filtering Services : No
Static Entry Individual Port         : Yes
VLAN Learning                       : IVL
Configurable PVID Tagging            : Yes
Local VLAN Capable                   : No
Traffic Classes                      : Enabled
Global GVRP Status                   : Disabled
GMRP                                 : Disabled
Console#
```

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: 1-28/52)
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 \(1121\)](#)

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: 1-28/52)
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 135: Commands for Editing VLAN Groups

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC

vlan database This command enters VLAN database mode. All commands in this mode will take effect immediately.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the [show vlan](#) command.
- ◆ Use the [interface vlan](#) command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the [show running-config](#) command.

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#
```

RELATED COMMANDS

[show vlan \(1134\)](#)

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: 1-4093)

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). For more information on configuring RSPAN through the CLI, see ["RSPAN Mirroring Commands" on page 1016](#).

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 4093 VLANs on the switch.



NOTE: The switch allows 4093 user-manageable VLANs.

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 \(1134\)](#)

CONFIGURING VLAN INTERFACES

Table 136: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport mode	Configures VLAN membership mode for an interface	IC
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC
switchport priority default	Sets a port priority for incoming untagged frames	IC
vlan-trunking	Allows unknown VLANs to cross the switch	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: 1-4093)

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` (979)
`interface` (974)
`vlan` (1126)

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 \(1131\)](#)

switchport allowed vlan This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

SYNTAX

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed 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: 1-4093).

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

- ◆ A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- ◆ If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- ◆ Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- ◆ If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

- ◆ If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

EXAMPLE

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport 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

Disabled

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)

COMMAND USAGE

Access mode is mutually exclusive with VLAN trunking (see the [vlan-trunking](#) command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

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 \(1128\)](#)

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: 1-4093)

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)#
```

vlan-trunking This command allows unknown VLAN groups to pass through the specified interface. Use the **no** form to disable this feature.

SYNTAX

[no] vlan-trunking

DEFAULT SETTING

Disabled

COMMAND MODE

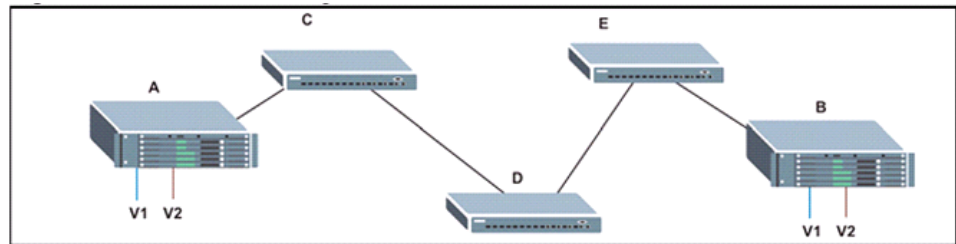
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ Use this command to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

Figure 431: Configuring VLAN Trunking



Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- ◆ VLAN trunking is mutually exclusive with the “access” switchport mode (see the [switchport mode](#) command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
- ◆ To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).
- ◆ If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

EXAMPLE

The following example enables VLAN trunking on ports 9 and 10 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/9
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/10
Console(config-if)#vlan-trunking
Console(config-if)#
```

DISPLAYING VLAN INFORMATION

This section describes commands used to display VLAN information.

Table 137: 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: 1-4093)

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) Eth1/27(S) Eth1/28(S)

Console#
```

CONFIGURING IEEE 802.1Q TUNNELING

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 138: 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 service match cvlan</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</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 \(1141\)](#)
[show interfaces switchport \(986\)](#)

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 \(1141\)](#)

[show interfaces switchport \(986\)](#)

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

svid - VLAN ID for the outer VLAN tag (Service Provider VID).
(Range: 1-4093)

cvid - VLAN ID for the inner VLAN tag (Customer VID).
(Range: 1-4093)

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 as described under ["IEEE 802.1Q Tunneling" on page 206](#).
- ◆ 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.

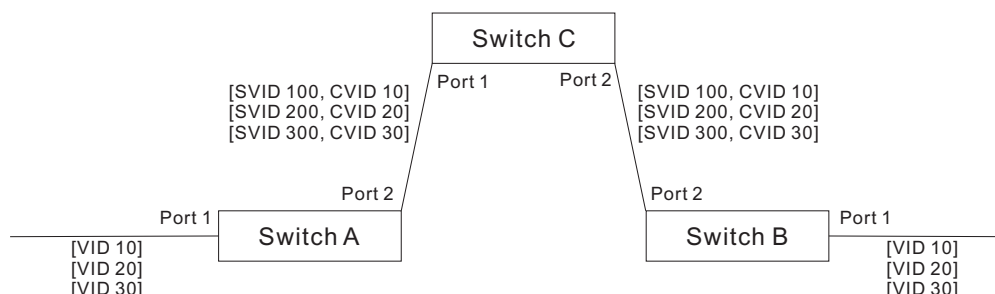
EXAMPLE

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 432: 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
Eth 1/ 1		10	100
Eth 1/ 1		20	200
Eth 1/ 1		30	300

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 processes 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 \(986\)](#)**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* - Stack unit. (Range: 1)*port* - Port number. (Range: 1-28/52)**port-channel** *channel-id* (Range: 1-16)*svid* - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4093)

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

Port      Mode    TPID (hex)
-----
Eth 1/ 1 Access      8100
Eth 1/ 2 Uplink      8100
Eth 1/ 3 Normal      8100
:
:
Console#show dot1q-tunnel interface ethernet 1/5
802.1Q Tunnel Service Subscriptions

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

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

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

Console#

```

RELATED COMMANDS

[switchport dot1q-tunnel mode \(1137\)](#)

CONFIGURING L2CP TUNNELING

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

Table 139: L2 Protocol Tunnel Commands

Command	Function	Mode
<code>l2protocol-tunnel tunnel-dmac</code>	Configures the destination address for Layer 2 Protocol Tunneling	GC
<code>switchport l2protocol-tunnel</code>	Enables Layer 2 Protocol Tunneling for the specified protocol	IC
<code>show l2protocol-tunnel</code>	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 01-12-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 ports³⁶ 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.
 - 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:

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

- 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 | lldp | pvst+ | spanning-tree | vtp}

cdp - Cisco Discovery 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 140: VLAN Translation Commands

Command	Function	Mode
<code>switchport vlan-translation</code>	Maps VLAN IDs between the customer and service provider	IC
<code>show vlan-translation</code>	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: 1-4093)

new-vlan - The new VLAN ID. (Range: 1-4093)

DEFAULT SETTING

Disabled

COMMAND MODE

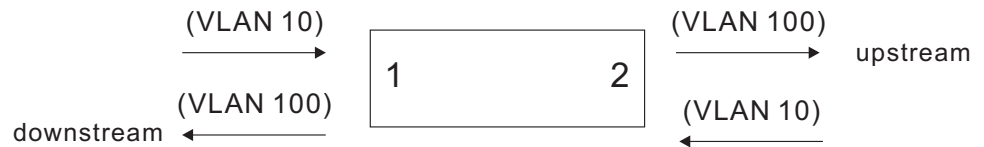
Interface Configuration (Ethernet)

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 433: 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 [**interface** *interface*]

interface

ethernet *unit/port*

unit - Stack unit. (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 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 141: Commands for Configuring Traffic Segmentation

Command	Function	Mode
traffic-segmentation	Enables traffic segmentation	GC
traffic-segmentation session	Creates a client session	GC
traffic-segmentation uplink/downlink	Configures uplink/downlink ports for client sessions	GC
traffic-segmentation uplink-to-uplink	Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions	GC
show traffic-segmentation	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 142: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured by the [traffic-segmentation uplink-to-uplink](#) command.

- ◆ When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.
- ◆ Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the [traffic-segmentation uplink/downlink](#) command.
- ◆ Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

EXAMPLE

This example enables traffic segmentation globally on the switch.

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session This command creates a traffic-segmentation client session. Use the **no** form to remove a client session.

SYNTAX

[no] traffic-segmentation session session-id
session-id – Traffic segmentation session. (Range: 1-4)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

Command Usage

- ◆ Use this command to create a new traffic-segmentation client session.
- ◆ Using the **no** form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

Example

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

traffic-segmentation uplink/downlink This command configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to remove a port from the segmented group.

SYNTAX

[no] traffic-segmentation [session session-id] {uplink interface-list [downlink interface-list] | downlink interface-list}

session-id – Traffic segmentation session. (Range: 1-4)

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

interface-list – One or more ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

Private VLAN Status      :      Enabled
Uplink-to-Uplink Mode    :      Forwarding

Session  Uplink Ports      Downlink Ports
-----
      1   Ethernet 1/1      Ethernet 1/2
                                Ethernet 1/3
                                Ethernet 1/4

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 143: 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 1126). 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*³⁷ - 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, ipv6.

DEFAULT SETTING

No protocol groups are configured.

COMMAND MODE

Global Configuration

³⁷. SNAP frame types are not supported by this switch due to hardware limitations.

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: 1-4093)

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.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the **vlan** command), these interfaces will admit traffic of any protocol type into the associated VLAN.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- ◆ When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
 - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
 - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.

- If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

EXAMPLE

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2 priority 0
Console(config-if)#
```

show protocol-vlan protocol-group This command shows the frame and protocol type associated with protocol groups.

SYNTAX

show protocol-vlan protocol-group [*group-id*]

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

DEFAULT SETTING

All protocol groups are displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

Protocol Group ID  Frame Type  Protocol Type
-----
                  1          ethernet    08 00
Console#
```

show interfaces protocol-vlan protocol-group This command shows the mapping from protocol groups to VLANs for the selected interfaces.

SYNTAX

show interfaces protocol-vlan protocol-group [*interface*]
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)
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      ProtocolGroup ID      VLAN ID
  -----
  Eth 1/1           1          vlan2
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 144: IP Subnet VLAN Commands

Command	Function	Mode
subnet-vlan	Defines the IP Subnet VLANs	GC
show subnet-vlan	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: 1-4093)

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, and 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 145: MAC Based VLAN Commands

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

mac-vlan This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

SYNTAX

mac-vlan mac-address *mac-address* **vlan** *vlan-id* [**priority** *priority*]

no mac-vlan mac-address {*mac-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.

vlan-id – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4093)

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.

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 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 146: Voice VLAN Commands

Command	Function	Mode
<code>voice vlan</code>	Defines the Voice VLAN ID	GC
<code>voice vlan aging</code>	Configures the aging time for Voice VLAN ports	GC
<code>voice vlan mac-address</code>	Configures VoIP device MAC addresses	GC
<code>switchport voice vlan</code>	Sets the Voice VLAN port mode	IC
<code>switchport voice vlan priority</code>	Sets the VoIP traffic priority for ports	IC
<code>switchport voice vlan rule</code>	Sets the automatic VoIP traffic detection method for ports	IC
<code>switchport voice vlan security</code>	Enables Voice VLAN security on ports	IC
<code>show voice vlan</code>	Displays Voice VLAN settings	PE

voice vlan This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

SYNTAX

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4093)

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.

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. (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
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 1269](#) 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

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      Enabled OUI                6 100
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#
```

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 147: 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 148: Priority Commands (Layer 2)

Command	Function	Mode
queue mode	Sets the queue mode to Weighted Round-Robin (WRR), strict priority, or a combination of strict and weighted queuing	GC
queue weight	Assigns round-robin weights to the priority queues	GC
switchport priority default	Sets a port priority for incoming untagged frames	IC
show interfaces switchport	Displays the administrative and operational status of an interface	PE
show queue mode	Shows the current queue mode	PE
show queue weight	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 queueing. 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 - Strict priority is used for the high-priority queues and WRR for the rest of the queues.

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

Global Configuration

COMMAND USAGE

- ◆ The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queueing.
- ◆ 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 queueing. Use the [queue weight](#) command to assign weights for WRR queueing to the eight priority queues.
- ◆ If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field 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.
- ◆ Protocols used to synchronize distributed switches use packets of 1588 bytes to control the synchronization process. This switch therefore assigns packets of this size to the highest priority queue to ensure quick passage.

EXAMPLE

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

RELATED COMMANDS

[queue weight \(1169\)](#)

[show queue mode \(1171\)](#)

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

Global Configuration

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 1168](#)).
- ◆ 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 - 4 to the CoS priority queues 0 - 7.

```
Console(config)#queue weight 1 2 3 4 5 6 7 8
Console(config)#
```

RELATED COMMANDS

[queue mode \(1168\)](#)

[show queue weight \(1171\)](#)

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 \(986\)](#)

show queue mode This command shows the current queue mode.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue mode

Queue Mode : Weighted Round Robin Mode
Console#
```

show queue weight This command displays the weights used for the weighted queues.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue weight
Queue ID  Weight
-----  -
          0          1
          1          2
          2          4
          3          6
          4          8
          5         10
          6         12
          7         14
Console#
```

PRIORITY COMMANDS (LAYER 3 AND 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 149: Priority Commands (Layer 3 and 4)

Command	Function	Mode
<code>qos map cos-dscp</code>	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
<code>qos map dscp-mutation</code>	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
<code>qos map phb-queue</code>	Maps internal per-hop behavior values to hardware queues	IC
<code>qos map trust-mode</code>	Sets QoS mapping to DSCP or CoS	IC
<code>show qos map cos-dscp</code>	Shows ingress CoS to internal DSCP map	PE
<code>show qos map dscp-mutation</code>	Shows ingress DSCP to internal DSCP map	PE
<code>show qos map phb-queue</code>	Shows internal per-hop behavior to hardware 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-dscp This command maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map cos-dscp *phb drop-precedence* **from** *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

phb - Per-hop behavior, or the priority used for this router hop.
(Range: 0-7)

drop-precedence - Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

cos - CoS value in ingress packets. (Range: 0-7)

cfi - Canonical Format Indicator. Set to 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 150: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS	CFI	0	1
0		(0,0)	(0,0)
1		(1,0)	(1,0)
2		(2,0)	(2,0)
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 (Port, Static Aggregation)

COMMAND USAGE

- ◆ The default mapping of CoS to PHB values shown in [Table 150](#) is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.
- ◆ Enter a value pair for the internal per-hop behavior and drop precedence, 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-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- ◆ The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used to control traffic congestion.
- ◆ The specified mapping applies to all interfaces.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map cos-dscp 0 0 from 0 1
Console(config-if)#
```

qos map dscp-mutation This command maps DSCP values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map dscp-mutation *phb drop-precedence* **from** *dscp0 ... dscp7*

no qos map dscp-mutation *dscp0 ... dscp7*

phb - Per-hop behavior, or the priority used for this router hop.
(Range: 0-7)

drop-precedence - Drop precedence used in controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

dscp - DSCP value in ingress packets. (Range: 0-63)

DEFAULT SETTING.

Table 151: Default Mapping of DSCP Values to Internal PHB/Drop Values

	ingress-dscp1	0	1	2	3	4	5	6	7	8	9
ingress-dscp10											
0		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 internal-dscp is shown at the intersecting cell in the table.

The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- ◆ Enter a value pair for the internal per-hop behavior and drop precedence, 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-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation

map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

- ◆ The specified mapping applies to all interfaces.

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 and a drop precedence of 1. Referring to [Table 151](#), note that the DSCP value for these packets is now set to 25 ($3 \times 2^3 + 1$) and passed on to the egress interface.

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-mutation 3 1 from 1
Console(config-if)#
```

qos map phb-queue This command determines the hardware output queues to use based on the internal per-hop behavior value. Use the **no** form to restore the default settings.

SYNTAX

qos map phb-queue *queue-id* **from** *phb0 ... phb7*

no map phb-queue *phb0 ... phb7*

phb - Per-hop behavior, or the priority used for this router hop.
(Range: 0-7)

queue-id - The ID of the priority queue. (Range: 0-7, where 7 is the highest priority queue)

DEFAULT SETTING.

Table 152: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	2	0	1	3	4	5	6	7

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- ◆ Enter a queue identifier, followed by the keyword "from" and then up to eight internal per-hop behavior values separated by spaces.
- ◆ Egress packets are placed into the hardware queues according to the mapping defined by this command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map phb-queue 0 from 1 2 3
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 (Port)

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 1170](#)) 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 1170](#)) 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 ge1/1
Console(config-if)#qos map trust-mode dscp
Console(config-if)#
```

show qos map cos-dscp This command shows ingress CoS/CFI to internal DSCP map.

SYNTAX

show qos map cos-dscp interface *interface*
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)
port-channel *channel-id* (Range: 1-16)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show qos map cos-dscp interface ethernet 1/5
CoS Information of Eth 1/5
CoS-DSCP map.(x,y),x: PHB,y: drop precedence:
CoS  : CFI   0           1
-----
0           (0,0)       (0,0)
1           (1,0)       (1,0)
2           (2,0)       (2,0)
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)
Console#
```

show qos map dscp-mutation This command shows the ingress DSCP to internal DSCP map.

SYNTAX

show qos map dscp-mutation interface *interface*
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)
port-channel *channel-id* (Range: 1-16)

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 “d1” (most significant digit in the left column) and “d2” (least significant digit in the top row (in other words, ingress DSCP = d1 * 10 + d2); and the corresponding Internal DSCP and drop precedence is shown at the intersecting cell in the table.

```
Console#show qos map dscp-mutation interface ethernet 1/5
Information of Eth 1/5
DSCP mutation map.(x,y),x: PHB,y: drop precedence:
d1: d2 0      1      2      3      4      5      6      7      8      9
-----
0 :      (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)
Console#
```

show qos map phb-queue This command shows internal per-hop behavior to hardware queue map.

SYNTAX

```
show qos map phb-queue interface interface
                                interface
                                ethernet unit/port
                                    unit - Unit identifier. (Range: 1)
                                    port - Port number. (Range: 1-28/52)
                                port-channel channel-id (Range: 1-16)
```

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
PHB-queue map:
PHB:      0      1      2      3      4      5      6      7
-----
Queue:    2      0      1      3      4      5      6      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: 1-28/52)

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#
```


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 153: 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 flow</code>	Defines an enforcer for classified traffic based on a metered flow rate	PM-C
<code>police srtcm-color</code>	Defines an enforcer for classified traffic based on a single rate three color meter	PM-C
<code>police trtcm-color</code>	Defines an enforcer for classified traffic based on a two rate three color meter	PM-C
<code>set cos</code>	Serves IP traffic by setting a class of service value for matching packets for internal processing	PM-C
<code>set ip dscp</code>	Serves IP traffic by setting a IP DSCP value for matching packets for internal processing	PM-C
<code>set phb</code>	Serves IP traffic by setting a per-hop behavior 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 incoming 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, a CoS value, or a source port.
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 phb**, **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* [**match-all** | **match-any**]
class-map-name - Name of the class map. (Range: 1-32 characters)
match-all - Match all conditions within a class map.
match-any - Match any condition within a class map.

DEFAULT SETTING

None

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 1186](#)). The policy map is then bound by a service policy to an interface ([page 1197](#)). 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 match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

RELATED COMMANDS

[show class-map \(1197\)](#)

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: 1-28/52)

vlan - A VLAN. (Range:1-4093)

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 match-any
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 match-any
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 match-any
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 1186](#)) 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, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
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 phb** command sets the per-hop behavior value in matching packets. (This modifies packet priority for internal processing only.)
 - **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 phb** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4,000 bytes, and configure the response to drop any violating packets.

```

Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#

```

police flow 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 flow committed-rate committed-burst
conform-action transmit
violate-action {drop | new-dscp}
```

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

conform-action - Action to take when packet is within the CIR and BC. (There are enough tokens to service the packet, the packet is set green).

violate-action - Action to take when packet exceeds the CIR and BC. (There are not enough tokens to service the packet, the packet is set red).

transmit - Transmits without taking any action.

drop - Drops packet as required by violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

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, and the *committed-burst* cannot exceed 16 Mbytes.
- ◆ Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *committed-burst* field, and the average rate tokens 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 $Tc(0) = BC$. Thereafter, the token count Tc is updated CIR times per second as follows:

- If Tc is less than BC , Tc is incremented by one, else
- Tc is not incremented.

When a packet of size B bytes arrives at time t , the following happens:

- If $Tc(t) - B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- else the packet is red and Tc 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 phb` command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

police srtcm-color This command defines an enforcer for classified traffic based on a single rate three color meter (srTCM). Use the **no** form to remove a policer.

SYNTAX

```
[no] police {srtcm-color-blind | srtcm-color-aware}
    committed-rate committed-burst excess-burst
    conform-action transmit
    exceed-action {drop | new-dscp}
    violate action {drop | new-dscp}
```

srtcm-color-blind - Single rate three color meter in color-blind mode.

srtcm-color-aware - Single rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

excess-burst - Excess burst size (BE) in bytes. (Range: 64-1600000 at a granularity of 4k bytes)

conform-action - Action to take when rate is within the CIR and BC. (There are enough tokens in bucket BC to service the packet, packet is set green).

exceed-action - Action to take when rate exceeds the CIR and BC but is within the BE. (There are enough tokens in bucket BE to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the BE. (There are not enough tokens in bucket BE to service the packet, the packet is set red.)

transmit - Transmits without taking any action.

drop - Drops packet as required by exceed-action or violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value.
(Range: 0-63)

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, and the *committed-burst* and *excess-burst* cannot exceed 16 Mbytes.
- ◆ The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – Committed Information Rate (CIR), Committed Burst Size (BC), and Excess Burst Size (BE).
- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green if it doesn't exceed the CIR and BC, yellow if it does exceed the CIR and BC, but not the BE, and red otherwise.
- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

The token buckets C and E are initially full, that is, the token count $T_c(0) = BC$ and the token count $T_e(0) = BE$. Thereafter, the token counts T_c and T_e are updated CIR times per second as follows:

- If T_c is less than BC , T_c is incremented by one, else
- if T_e is less than BE , T_e is incremented by one, else
- neither T_c nor T_e is incremented.

When a packet of size B bytes arrives at time t , the following happens if srTCM is configured to operate in color-blind mode:

- 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
- if $T_e(t) - B \geq 0$, the packet is yellow and T_e is decremented by B down to the minimum value of 0,
- else the packet is red and neither T_c nor T_e is decremented.

When a packet of size B bytes arrives at time t , the following happens if srTCM is configured to operate in color-aware mode:

- If the packet has been precolored as green and $T_c(t) - B \geq 0$, the packet is green and T_c is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if
- $T_e(t) - B \geq 0$, the packet is yellow and T_e is decremented by B down to the minimum value of 0, else the packet is red and neither T_c nor T_e is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC , that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

EXAMPLE

This example creates a policy called "rd-policy," uses the `class` command to specify the previously defined "rd-class," uses the `set phb` command to classify the service that incoming packets will receive, and then uses the **police srtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the excess burst rate to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the excess burst size.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-
  action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

police trtcm-color This command defines an enforcer for classified traffic based on a two rate three color meter (trTCM). Use the **no** form to remove a policer.

SYNTAX

```
[no] police {trtcm-color-blind | trtcm-color-aware}
        committed-rate committed-burst peak-rate peak-burst
        conform-action transmit
        exceed-action {drop | new-dscp}
        violate action {drop | new-dscp}
```

trtcm-color-blind - Two rate three color meter in color-blind mode.

trtcm-color-aware - Two rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

peak-rate - Peak information rate (PIR) in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

peak-burst - Peak burst size (BP) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

conform-action - Action to take when rate is within the CIR and BP. (Packet size does not exceed BP and there are enough tokens in bucket BC to service the packet, the packet is set green.)

exceed-action - Action to take when rate exceeds the CIR but is within the PIR. (Packet size exceeds BC but there are enough tokens in bucket BP to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the PIR. (There are not enough tokens in bucket BP to service the packet, the packet is set red.)

drop - Drops packet as required by exceed-action or violate-action.

transmit - Transmits without taking any action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

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* and *peak-rate* cannot exceed the configured interface speed, and the *committed-burst* and *peak-burst* cannot exceed 16 Mbytes.
- ◆ The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – Committed Information Rate (CIR) and Peak Information Rate (PIR), and their associated burst sizes - Committed Burst Size (BC) and Peak Burst Size (BP).
- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.
- ◆ The token buckets P and C are initially (at time 0) full, that is, the token count $Tp(0) = BP$ and the token count $Tc(0) = BC$. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:

- If $Tp(t) - B < 0$, the packet is red, else
- if $Tc(t) - B < 0$, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:

- If the packet has been precolored as red or if $Tp(t) - B < 0$, the packet is red, else
- if the packet has been precolored as yellow or if $Tc(t) - B < 0$, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.
- ◆ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

EXAMPLE

This example creates a policy called "rd-policy," uses the `class` command to specify the previously defined "rd-class," uses the `set phb` command to classify the service that incoming packets will receive, and then uses the **police trtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000
    conform-action transmit exceed-action 0 violate-action drop
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.
- ◆ The **set cos** and `set phb` command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

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 flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
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
violate-action drop
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 flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
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 flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

set phb This command services IP traffic by setting a per-hop behavior value for a matching packet (as specified by the [match](#) command) for internal processing. Use the **no** form to remove this setting.

SYNTAX

[no] set phb *phb-value*

phb-value - Per-hop behavior value. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- ◆ The **set phb** command is used to set an internal QoS value in hardware for matching packets (see [Table 151, "Default Mapping of DSCP Values to Internal PHB/Drop Values"](#)). The QoS label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion by the [police srtcm-color](#) command and [police trtcm-color](#) command.
- ◆ The [set cos](#) and **set phb** command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

EXAMPLE

This example creates a policy called "rd-policy," uses the [class](#) command to specify the previously defined "rd-class," uses the **set phb** command to classify the service that incoming packets will receive, and then uses the [police flow](#) command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
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.

output - Apply to the output 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 incoming 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
Console#show policy-map rd-policy 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: 1-28/52)
port-channel *channel-id* (Range: 1-16)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```


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 154: 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
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 155: 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
<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

Table 155: IGMP Snooping Commands (Continued)

Command	Function	Mode
<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>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: 1-4093)

DEFAULT SETTING

Enabled

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: 0-6, where 6 is the highest priority)

DEFAULT SETTING

2

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 \(1218\)](#)

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: 1-4093)

enable - Enable on the specified VLAN.

disable - Disable on the specified VLAN.

DEFAULT SETTING

Global: Enabled

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

Enabled

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 time out. 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 time out 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 time out 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 issue 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 version-exclusive

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 1204](#)).

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: 1-4093)

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: 1-4093)

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: 1-4093)

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

[no] ip igmp snooping vlan *vlan-id* immediate-leave

vlan-id - VLAN ID (Range: 1-4093)

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 time out period. (The time out for this release is currently defined by Last Member Query Interval (fixed at one second) * Robustness Variable (fixed at 2) as defined in RFC 2236.
- ◆ If 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 IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- ◆ 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: 1-4093)

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 1204](#)).

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: 1-4093)

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 1204](#)).

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: 1-4093)

DEFAULT SETTING

Enabled

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: 1-4093)

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: 1-4093)

interval - The interval between sending IGMP general queries.
(Range: 10-31744 seconds)

DEFAULT SETTING

100 (10 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 1205](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 1204](#)).

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: 1-4093)

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 1205](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 1204](#)).

EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```

ip igmp snooping This command adds a port to a multicast group. Use the **no** form to
vlan static remove the port.

SYNTAX

[no] ip igmp snooping vlan *vlan-id* static *ip-address* *interface*

vlan-id - VLAN ID (Range: 1-4093)

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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)#
```

show ip igmp This command shows the IGMP snooping, proxy, and query configuration
snooping settings.

SYNTAX

show ip igmp snooping [*vlan* *vlan-id*]

vlan-id - VLAN ID (1-4093)

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays global and VLAN-specific IGMP configuration settings. See ["Configuring IGMP Snooping and Query Parameters" on page 560](#) for a description of the displayed items.

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
TCN Flood                                  : Disabled
TCN Query Solicit                          : Disabled
Unregistered Data Flood                    : Disabled
802.1p Forwarding Priority                  : 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: 1-28/52)

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 (1-4093)

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		00:00:00:37	2 (P)
	Eth 1/ 1 (R)		
	Eth 1/ 2 (M)		0 (H)

Console#

show ip igmp snooping mrouter This command displays information on dynamically learned and statically configured multicast router ports.

SYNTAX

show ip igmp snooping mrouter [**vlan** *vlan-id*]
vlan-id - VLAN ID (Range: 1-4093)

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 Ports 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: 1-28/52)
port-channel *channel-id* (Range: 1-16)
vlan *vlan-id* - VLAN ID (Range: 1-4093)
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
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 156: 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
-----
Eth 1/ 1           12         0         1         0
Console#
```

Table 157: show ip igmp snooping statistics output - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows IGMP query-related statistics for VLAN 1:

```

Console#show ip igmp snooping statistics query vlan 1
Querier IP Address      : 192.168.1.1
Querier Expire Time     : 00:00:30
General Query Received  : 10
General Query Sent      : 0
Specific Query Received : 2
Specific Query Sent     : 0
Number of Reports Sent  : 2
Number of Leaves Sent   : 0
Console#

```

Table 158: show ip igmp snooping statistics vlan query - display description

Field	Description
Querier IP Address	The IP address of the querier on this interface.
Querier Expire Time	The time after which this querier is assumed to have expired.
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.
Number of Reports Sent	The number of reports sent from this interface.
Number of Leaves Sent	The number of leaves sent from this interface.

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routing on the switch.

Table 159: 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 This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.
vlan mrouter

SYNTAX

[no] ip igmp snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4093)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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 160: IGMP Filtering and Throttling Commands

Command	Function	Mode
<code>ip igmp filter</code>	Enables IGMP filtering and throttling on the switch	GC
<code>ip igmp profile</code>	Sets a profile number and enters IGMP filter profile configuration mode	GC
<code>permit, deny</code>	Sets a profile access mode to permit or deny	IPC
<code>range</code>	Specifies one or a range of multicast addresses for a profile	IPC
<code>ip igmp filter</code>	Assigns an IGMP filter profile to an interface	IC
<code>ip igmp max-groups</code>	Specifies an IGMP throttling number for an interface	IC
<code>ip igmp max-groups action</code>	Sets the IGMP throttling action for an interface	IC
<code>ip igmp query-drop</code>	Drops any received IGMP query packets	IC
<code>show ip igmp filter</code>	Displays the IGMP filtering status	PE
<code>show ip igmp profile</code>	Displays IGMP profiles and settings	PE
<code>show ip igmp query-drop</code>	Shows if the interface is configured to drop IGMP query packets	PE
<code>show ip igmp throttle interface</code>	Displays the IGMP throttling setting for interfaces	PE

ip igmp filter (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 filter This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.
(Interface Configuration)

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: 1-1023)

DEFAULT SETTING

1023

COMMAND MODE

Interface Configuration (Ethernet)

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)

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)

COMMAND USAGE

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

show ip igmp filter This command displays the global and interface settings for IGMP filtering.

SYNTAX

show ip igmp filter [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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 - Stack unit. (Range: 1)

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

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: 1-28/52)

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 : TRUE
  Action : Deny
  Max Multicast Groups : 32
  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 161: 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>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
<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

Table 161: Multicast VLAN Registration for IPv4 Commands (Continued)

Command	Function	Mode
<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 \(1235\)](#)

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 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*

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 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: 0-6, where 6 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 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 \(1239\)](#)

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 \(1237\)](#)

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: 1-4093)

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

[**no**] **mvr** [**domain** *domain-id*] **immediate-leave**

domain-id - An independent multicast domain. (Range: 1-5)

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.
- ◆ 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: 1-4093)

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)#
```

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 162: 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	The interval at which the receiver port sends out general queries
MVR Source Port Mode	Shows if the switch only forwards multicast streams which the source port has dynamically joined or always forwards multicast streams
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.)
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
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)
Eth1/ 3 Source  Inactive/Discarding
Eth1/ 1 Receiver Active/Forwarding Disabled    225.0.0.1 (VLAN1)
                                           225.0.0.9 (VLAN3)
Eth1/ 4 Receiver Active/Discarding Disabled
Console#
```

Table 163: 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.

Table 163: show mvr interface - display description (Continued)

Field	Description
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*] | **sort-by-port** [*interface*]]]

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.

sort-by-port - The multicast groups associated with an interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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		2 (P)
	1 Eth 1/ 1(S)		
	2 Eth 1/ 2(R)		

Console#

Table 164: 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 statistics {input | output} [interface *interface*]

show mvr 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: 1-28/52)

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

vlan *vlan-id* - VLAN ID (Range: 1-4093)

query - Displays MVR query-related 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
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
VLAN    1           2        0        0          2       2       20       9
Console#

```

Table 165: 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.
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
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
VLAN    1           7        2        3          0
Console#

```

Table 166: 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.

Table 166: show mvr statistics output - display description (Continued)

Field	Description
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.

The following shows MVR query-related statistics:

```

Console#show mvr domain 1 statistics query
Querier IP Address      : 192.168.1.1
Querier Expire Time     : 00:00:30
General Query Received  : 10
General Query Sent      : 0
Specific Query Received : 2
Specific Query Sent     : 0
Number of Reports Sent  : 2
Number of Leaves Sent   : 0
Console#

```

Table 167: show mvr statistics query - display description

Field	Description
Querier IP Address	The IP address of the querier on this interface.
Querier Expire Time	The time after which this querier is assumed to have expired.
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.
Number of Reports Sent	The number of reports sent from this interface.
Number of Leaves Sent	The number of leaves sent from this interface.

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 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 168: Multicast VLAN Registration for IPv6 Commands

Command	Function	Mode
<code>mvr6 associated-profile</code>	Binds the MVR group addresses specified in a profile to an MVR domain	GC
<code>mvr6 domain</code>	Enables MVR for a specific domain	GC
<code>mvr6 profile</code>	Maps a range of MVR 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 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>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 MVR multicast data is received	GC
<code>mvr6 immediate-leave</code>	Enables immediate leave capability	IC
<code>mvr6 type</code>	Configures an interface as an MVR receiver or source port	IC
<code>mvr6 vlan group</code>	Statically binds a multicast group to a port	IC
<code>show mvr6</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 mvr6 associated-profile</code>	Shows the profiles bound the specified domain	PE
<code>show mvr6 interface</code>	Shows MVR settings for interfaces attached to the MVR VLAN	PE
<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 MVR profiles	PE
<code>show mvr6 statistics</code>	Shows MVR protocol statistics for the specified interface	PE

mvr6 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] 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 MVR 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 MVR group address profile to domain 1:

```
Console(config)#mvr6 domain 1 associated-profile rd
Console(config)#
```

mvr6 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] 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 MVR for domain 1:

```
Console(config)#mvr6 domain 1
Console(config)#
```

mvr6 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

mvr6 profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv6 address for an MVR 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 MVR 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 MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.
- ◆ 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 MVR group addresses to a profile:

```
Console(config)#mvr6 profile rd ff00::1 ff00::9
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

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 [mvr6 proxy-switching](#) command.

EXAMPLE

This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```

mvr6 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] mvr6 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, and the MVR receiver port serves as the querier. 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)#
```

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 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 MVR6 proxy switching is enabled.

EXAMPLE

```
Console(config)#mvr6 robustness-value 5
Console(config)#
```

RELATED COMMANDS

[mvr6 proxy-switching \(1255\)](#)

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 MVR 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 MVR control packets sent upstream. This parameter must be a full IPv6 address including the network prefix and host address bits.

DEFAULT SETTING

All MVR 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 MVR multicast data is received. Use the **no** form of this command to restore the default MVR 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 MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4093)

DEFAULT SETTING

VLAN 1

COMMAND MODE

Global Configuration

COMMAND USAGE

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 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

domain-id - An independent multicast domain. (Range: 1-5)

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.
- ◆ 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 MVR 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.
- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of 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 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 MVR 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: 1-4093)

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 MVR 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 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 1/2
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1
Console(config-if)#
```

show mvr6 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 mvr6 [**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 mvr6
MVR6 Proxy Switching      : Enabled
MVR6 Robustness Value     : 1

MVR6 Domain               : 1
MVR6 Config Status        : Enabled
MVR6 Running Status       : Active
MVR6 Multicast VLAN       : 1
MVR6 Upstream Source IP   : FF05::25
Console#
```

Table 169: show mvr6 - display description

Field	Description
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
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 mvr6 type command.)

Table 169: show mvr6 - display description (Continued)

Field	Description
MVR6 Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
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 MVR 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
MVR Profile Name      Start IPv6 Addr.      End IPv6 Addr.
-----
rd                     FF00::1                FF00::9
Console#

```

show mvr6 interface This command shows MVR configuration settings for interfaces attached to the MVR 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 MVR VLAN in domain 1:

```
Console#show mvr6 domain 1 interface
MVR6 Domain : 1
Port      Type      Status      Immediate  Static Group Address
-----
Eth1/ 1   Source   Active/Up
Eth1/ 2   Receiver Active/Up   Disabled   FF00::1 (VLAN2)
Console#
```

Table 170: show mvr6 interface - display description

Field	Description
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.
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 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 MVR 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 ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address	VLAN	Port	Up time	Expire	Count
FF00::1		1			2 (P)
	1	Eth1/ 1(S)			
	2	Eth1/ 2(S)			

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 ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address	VLAN	Port	Up time	Expire	Count
FF00::1		1			2 (P)
	1	Eth1/ 1(S)			
	2	Eth1/ 2(S)			

Console#

Table 171: 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 MVR profiles.

SYNTAX

show mvr6 profile

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows all configured MVR profiles:

```
Console#show mvr6 profile
MVR Profile Name      Start IPv6 Addr.      End IPv6 Addr.
-----
rd                    FF00::1                FF00::9
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: 1-28/52)

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

vlan *vlan-id* - VLAN ID (Range: 1-4093)

query - Displays MVR query-related statistics.

DEFAULT SETTING

Displays statistics for all domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MVR 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
VLAN 1           2        0         0              2          2         20         9
Console#
```

Table 172: 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.
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 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
VLAN    1           7         2         3         0
Console#

```

Table 173: 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.

The following shows MVR query-related statistics:

```

Console#show mvr6 domain 1 statistics query
Querier IPv6 Address      : FE80::2E0:CFF:FE00:FB/64
Querier Expire Time       : 00(h):00(m):30(s)
General Query Received    : 10
General Query Sent        : 0
Specific Query Received   : 2
Specific Query Sent       : 0
Number of Reports Sent    : 2
Number of Leaves Sent     : 0
Console#

```


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 174: 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
<code>lldp basic-tlv system-description</code>	Configures an LLDP-enabled port to advertise the system description	IC

Table 174: LLDP Commands (Continued)

Command	Function	Mode
<code>lldp basic-tlv system-name</code>	Configures an LLDP-enabled port to advertise its system name	IC
<code>lldp dot1-tlv proto-ident*</code>	Configures an LLDP-enabled port to advertise the supported protocols	IC
<code>lldp dot1-tlv proto-vid*</code>	Configures an LLDP-enabled port to advertise port-based protocol related VLAN information	IC
<code>lldp dot1-tlv pvid*</code>	Configures an LLDP-enabled port to advertise its default VLAN ID	IC
<code>lldp dot1-tlv vlan-name*</code>	Configures an LLDP-enabled port to advertise its VLAN name	IC
<code>lldp dot3-tlv link-agg</code>	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC
<code>lldp dot3-tlv mac-phy</code>	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC
<code>lldp dot3-tlv max-frame</code>	Configures an LLDP-enabled port to advertise its maximum frame size	IC
<code>lldp dot3-tlv poe</code>	Configures an LLDP-enabled port to advertise its Power-over-Ethernet capabilities	IC
<code>lldp med-location civic-addr</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-notification</code>	Enables the transmission of SNMP trap notifications about LLDP-MED changes	IC
<code>lldp med-tlv ext-poe</code>	Configures an LLDP-MED-enabled port to advertise its extended Power over Ethernet configuration and usage information	IC
<code>lldp med-tlv inventory</code>	Configures an LLDP-MED-enabled port to advertise its inventory identification details	IC
<code>lldp med-tlv location</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-tlv med-cap</code>	Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities	IC
<code>lldp med-tlv network-policy</code>	Configures an LLDP-MED-enabled port to advertise its network policy configuration	IC
<code>lldp notification</code>	Enables the transmission of SNMP trap notifications about LLDP changes	IC
<code>show lldp config</code>	Shows LLDP configuration settings for all ports	PE
<code>show lldp info local-device</code>	Shows LLDP global and interface-specific configuration settings for this device	PE
<code>show lldp info remote-device</code>	Shows LLDP global and interface-specific configuration settings for remote devices	PE
<code>show lldp info statistics</code>	Shows statistical counters for all LLDP-enabled interfaces	PE

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

SYNTAX

[no] lldp

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

SYNTAX

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule:
minimum of ((Transmission Interval * Holdtime Multiplier), or 65536)

(Range: 2 - 10)

DEFAULT SETTING

Holdtime multiplier: 4

TTL: 4*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.

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)#
```

Ildp refresh-interval This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

SYNTAX

Ildp refresh-interval *seconds*

no Ildp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

DEFAULT SETTING

30 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

Ildp reinit-delay This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

SYNTAX

Ildp reinit-delay *seconds*

no Ildp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP. (Range: 1 - 10 seconds)

DEFAULT SETTING

2 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

EXAMPLE

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

SYNTAX

lldp tx-delay *seconds*

no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

DEFAULT SETTING

2 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.
- ◆ This attribute must comply with the following rule:
 $(4 * \text{tx-delay}) \leq \text{refresh-interval}$

EXAMPLE

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

SYNTAX

lldp admin-status {rx-only | tx-only | tx-rx}

no lldp admin-status

rx-only - Only receive LLDP PDUs.

tx-only - Only transmit LLDP PDUs.

tx-rx - Both transmit and receive LLDP Protocol Data Units (PDUs).

DEFAULT SETTING

tx-rx

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp basic-tlv management-ip-address This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

SYNTAX

[no] lldp basic-tlv management-ip-address

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- ◆ The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating

enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

- ◆ Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- ◆ Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

SYNTAX

[no] lldp basic-tlv port-description

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```


lldp basic-tlv system-capabilities This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

SYNTAX

[no] lldp basic-tlv system-capabilities

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

SYNTAX

[no] lldp basic-tlv system-description

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

SYNTAX

[no] lldp basic-tlv system-name

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the [hostname](#) command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

SYNTAX

[no] lldp dot1-tlv proto-ident

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the protocols that are accessible through this interface.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid This command configures an LLDP-enabled port to advertise port-based protocol VLAN information. Use the **no** form to disable this feature.

SYNTAX

[no] lldp dot1-tlv proto-vid

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the port-based protocol VLANs configured on this interface (see ["Configuring Protocol-based VLANs" on page 1152](#)).

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 1129](#) and ["protocol-vlan protocol-group \(Configuring Interfaces\)" on page 1154](#).

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

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Refer to ["Frame Size" on page 733](#) for information on configuring the maximum frame size for this switch.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe This command configures an LLDP-enabled port to advertise its Power-over-Ethernet (PoE) capabilities. Use the **no** form to disable this feature.

SYNTAX

[no] lldp dot3-tlv poe

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ This command only applies to the ECS4510-28P/52P.
- ◆ This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

lldp med-location civic-addr This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to restore the default settings.

SYNTAX

lldp med-location civic-addr **[[country country-code] | [what device-type] | [ca-type ca-value]]**

no lldp med-location civic-addr **[[country] | [what] | [ca-type]]**

country-code – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

device-type – The type of device to which the location applies.

0 – Location of DHCP server.

1 – Location of network element closest to client.

2 – Location of client.

ca-type – A one-octet descriptor of the data civic address value. (Range: 0-255)

ca-value – Description of a location. (Range: 1-32 characters)

DEFAULT SETTING

Not advertised
No description

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ Use this command without any keywords to advertise location identification details.
- ◆ Use the *ca-type* to advertise the physical location of the device, that is the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 175: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

- ◆ For the location options defined for *device-type*, normally option **2** is used to specify the location of the client device. In situations where the client device location is not known, **0** and **1** can be used, providing the client device is physically close to the DHCP server or network element.

EXAMPLE

The following example enables advertising location identification details.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
```

```

Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 6 Exchange
Console(config-if)#lldp med-location civic-addr 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#

```

lldp med-notification This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

SYNTAX

[no] lldp med-notification

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the [lldp notification-interval](#) command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the [snmp-server host](#) command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

EXAMPLE

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#

```


lldp med-tlv ext-poe This command configures an LLDP-MED-enabled port to advertise and accept Extended Power-over-Ethernet configuration and usage information. Use the **no** form to disable this feature.

SYNTAX

[no] **lldp med-tlv ext-poe**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ This command only applies to the ECS4510-28P/52P.
- ◆ This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode). Note that this device does not support PoE capabilities.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv ext-poe
Console(config-if)#
```

lldp med-tlv inventory This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

SYNTAX

[no] **lldp med-tlv inventory**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

EXAMPLE

```

Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#

```

lldp med-tlv location This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

SYNTAX

[no] lldp med-tlv location

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises location identification details.

EXAMPLE

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#

```

lldp med-tlv med-cap This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the **no** form to disable this feature.

SYNTAX

[no] lldp med-tlv med-cap

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

EXAMPLE

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#

```

lldp med-tlv network-policy This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the **no** form to disable this feature.

SYNTAX

[no] lldp med-tlv network-policy

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

EXAMPLE

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#

```

lldp notification This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

SYNTAX

[no] lldp notification

DEFAULT SETTING

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), 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: 1-28/52)

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

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp config

LLDP Global Configuration

LLDP Enabled                : Yes
LLDP Transmit Interval      : 30 sec.
LLDP Hold Time Multiplier   : 4
LLDP Delay Interval         : 2 sec.
LLDP Re-initialization Delay : 2 sec.
LLDP Notification Interval   : 5 sec.
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
  *poe
  *link-agg
  *max-frame
MED Configuration:
MED Notification Status : Enabled
MED Enabled TLVs Advertised:
  *med-cap
  *network-policy
  *location
  *extPoe
  *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: 1-28/52)

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

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show lldp info local-device

LLDP Local System Information
Chassis Type : MAC Address
Chassis ID   : 00-01-02-03-04-05
System Name  :
System Description : ECS4510-28T
System Capabilities Support : Bridge
System Capabilities Enable  : Bridge
Management Address : 192.168.0.101 (IPv4)

LLDP Port Information
Port      PortID Type      PortID      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 Port Information Details

Port          : Eth 1/1
Port Type     : MAC Address
Port ID       : 00-12-CF-DA-FC-E9
Port Description : Ethernet Port on unit 0, 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 configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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
```

Interface	Chassis ID	Port ID	System Name
Eth 1/1	00-E0-0C-00-00-FD	00-E0-0C-00-01-02	

```
Console#show lldp info remote-device detail ethernet 1/1
```

```
-----
Local Port Name      : Eth 1/2
Chassis Type         : MAC Address
Chassis ID           : 70-72-CF-18-B7-E0
Port ID Type         : MAC Address
Port ID              : 70-72-CF-18-B7-E1
System Name          :
System Description   : ECS4510-28T
Port Description     : Ethernet Port on unit 0, port 1
SystemCapSupported   : Bridge
SystemCapEnabled     : Bridge
Remote Management Address :
    192.168.0.5 (IPv4)
Remote Port VID      : 1
Remote Port-Protocol VLAN :
    VLAN-3 : supported, enabled
Remote VLAN Name     :
    VLAN-1 : DefaultVlan
Remote Protocol Identity (Hex) :
    88-CC
Remote MAC/PHY Configuration Status :
    Remote port auto-neg supported : Yes
    Remote port auto-neg enabled : Yes
    Remote port auto-neg advertised cap (Hex) : 0000
    Remote port MAU type : 6
Remote Power via MDI :
    Remote power class : PSE
    Remote power MDI supported : Yes
    Remote power MDI enabled : Yes
    Remote power pair controllable : No
    Remote power pairs : Spare
    Remote power classification : Class1
Remote Link Aggregation :
    Remote link aggregation capable : Yes
    Remote link aggregation enable : No
    Remote link aggregation port ID : 0
Remote Max Frame Size : 1518
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        : R01
  Firmware Revision       : 1.2.2.1
  Software Revision       : 1.2.2.1
  Serial Number           : LN10230092
  Manufacture Name        :
  Model Name              :
  Asset ID                :

```

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: 1-28/52)

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

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info statistics
```

```
LLDP Device Statistics
```

```
Neighbor Entries List Last Updated : 2450279 seconds
New Neighbor Entries Count          : 1
Neighbor Entries Deleted Count      : 0
Neighbor Entries Dropped Count      : 0
Neighbor Entries Ageout Count       : 0
```

Port	NumFramesRecvd	NumFramesSent	NumFramesDiscarded
Eth 1/1	0	83	0
Eth 1/2	11	12	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
```

```
PortName          : Eth 1/1
Frames Discarded  : 0
Frames Invalid    : 0
Frames Received   : 12
Frames Sent       : 13
TLVs Unrecognized : 0
TLVs Discarded    : 0
Neighbor Ageouts  : 0
```

```
Console#
```


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 176: 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
<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

Table 176: CFM Commands (Continued)

Command	Function	Mode
<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
<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

Table 176: CFM Commands (Continued)

Command	Function	Mode
<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 1315](#)), or setting the start-up delay for the cross-check operation ([page 1321](#)). You can also enable SNMP traps for events discovered by continuity check messages ([page 1317](#)) or cross-check messages ([page 1321](#)).

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 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. (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)#
```

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 \(1304\)](#)

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-id* [**mip-creation** *type*]]

no ma index *index* [**vlan** *vlan-id*]

index – MA identifier. (Range: 1-2147483647)

ma-name – MA name. (Range: 1-43 alphanumeric characters)

vlan-id – Service VLAN ID. (Range: 1-4093)

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.
- ◆ 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)

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

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 177: 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 ethernet cfm mep command), manually configured as a remote MEP (see the mep crosscheck mpid 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)
port - Port number. (Range: 1-28/52)
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)

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

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 178: 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 179: 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

Table 179: show ethernet cfm maintenance-points remote detail - display

Field	Description
CC Packet Statistics (received/error)	The number of CCM packets received successfully and those with errors
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 nor 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 sec, 5 - 10 sec, 6 - 1 min, 7 - 10 min).

DEFAULT SETTING

4 (1 sec)

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 \(1316\)](#)

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 \(1323\)](#)

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 180: 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	Error types include: 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. 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. EXCESS_LEV – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities. 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.
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 configured 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* [**ttl** *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: 1-255 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 181: 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.

Table 181: show ethernet cfm linktrace-cache - display description

Field	Description
Ing. Action	<p>Action taken on the ingress port:</p> <p>IngOk – The target data frame passed through to the MAC Relay Entity.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Egr. Action	<p>Action taken on the egress port:</p> <p>EgrOk – The targeted data frame was forwarded.</p> <p>EgrDown – The Egress Port can be identified, but that bridge port's MAC_Operational parameter is false.</p> <p>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.</p> <p>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.</p>
Relay	<p>Relay action:</p> <p>FDB – Target address found in forwarding database.</p> <p>MPDB – Target address found in the maintenance point database.</p> <p>HIT – Target located on this device.</p>

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 182: 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 183: 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 184: 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 mep fault-notify lowest-priority command).
Alarm Time	The time a defect must exist before a fault alarm is issued (see the mep fault-notify alarm-time , 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 mep fault-notify reset-time 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 TxTimestampb (Timestamp at the time of transmitting a frame with DM reply information):

$$\text{Frame Delay} = (\text{RxTimeStampb} - \text{TxTimeStampf}) - (\text{TxTimestampb} - \text{RxTimeStampf})$$
- ◆ 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#

```


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 185: 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>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

[no] efm oam link-monitor frame threshold *count*

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 ([page 1340](#)). 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

[no] efm oam link-monitor frame window *size*

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 ([page 1339](#)) 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: 1-28/52)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear efm oam counters
Console#
```

RELATED COMMANDS

[show efm oam counters interface \(1344\)](#)

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: 1-28/52)

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 ([page 1343](#)) 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: 1-28/52)

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: 1-28/52)

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: 1-28/52)

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#

```

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: 1-28/52)

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: 1-28/52)

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: 1-28/52)

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
   Address              Loopback Unidirectional Monitor Retrieval
-----
1/1  00-12-CF-6A-07-F6  000084 Enabled Disabled Enabled Disabled
Console#

```

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 186: Address Table Commands

Command	Function	Mode
ip domain-list	Defines a list of default domain names for incomplete host names	GC
ip domain-lookup	Enables DNS-based host name-to-address translation	GC
ip domain-name	Defines a default domain name for incomplete host names	GC
ip host	Creates a static IPv4 host name-to-address mapping	GC
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC
ipv6 host	Creates a static IPv6 host name-to-address mapping	GC
clear dns cache	Clears all entries from the DNS cache	PE
clear host	Deletes entries from the host name-to-address table	PE
show dns	Displays the configuration for DNS services	PE
show dns cache	Displays entries in the DNS cache	PE
show hosts	Displays the static host name-to-address mapping table	PE

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 \(1349\)](#)

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 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 \(1349\)](#)

[ip name-server \(1351\)](#)

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 \(1347\)](#)

[ip name-server \(1351\)](#)

[ip domain-lookup \(1348\)](#)

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: 1-100 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
    10.1.0.55
Console#
```

RELATED COMMANDS

[ip domain-name \(1349\)](#)

[ip domain-lookup \(1348\)](#)

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: 1-100 characters)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

DEFAULT SETTING

No static entries

COMMAND MODE

Global Configuration

EXAMPLE

This example maps an IPv6 address to a host name.

```

Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts

```

No.	Flag	Type	IP Address	TTL	Domain
0	2	Address	192.168.1.55		rd5
1	2	Address	2001:DB8:1::12		rd6

```

Console#

```

clear dns cache This command clears all entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#clear dns cache
Console#show dns cache

```

No.	Flag	Type	IP Address	TTL	Domain
-----	------	------	------------	-----	--------

```

Console#

```

clear host This command deletes dynamic entries from the DNS table.

SYNTAX

clear host {*name* | *}

name - Name of the host. (Range: 1-100 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(config)#clear host *
Console(config)#
```

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 187: 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      Domain
-----
  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.wal.b.yahoo.com
  4   4 CNAME  POINTER TO:3          65     www.yahoo.com
  5   4 CNAME  POINTER TO:3          65     www.wal.b.yahoo.com
Console#
```

Table 188: 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.
Domain	The domain name associated with this record.

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 189: 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 190: DHCP Client Commands

Command	Function	Mode
<i>DHCP for IPv4</i>		
<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
<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 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 option 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

None

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 191: 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 192: 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 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 \(1359\)](#)

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
Console#
```

RELATED COMMANDS

[ip address \(1368\)](#)

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: 1-4093; 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.

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: 1-4093; 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 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 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 \(1381\)](#)

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.
- ◆ To display the DUID assigned to this device, first enter the [ipv6 address autoconfig](#) command.

EXAMPLE

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
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-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: 1-4093; Maximum command length: 300 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode, Rapid-Commit
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#
```

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: 1-4093, no leading zeroes)

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 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

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

DHCP RELAY

This section describes commands used to configure the switch to relay DHCP requests from local hosts to a remote DHCP server.

Table 193: DHCP Relay Option 82 Commands

Command	Function	Mode
<code>ip dhcp relay server</code>	Specifies DHCP server or relay server addresses	IC
<code>ip dhcp restart relay</code>	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)#ip dhcp relay server 192.168.10.19
Console(config)#
```

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
Console#
```

RELATED COMMANDS

[ip dhcp relay server \(1364\)](#)

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 194: IP Interface Commands

Command Group	Function
IPv4 Interface	Configures an IPv4 address for the switch
IPv6 Interface	Configures an IPv6 address for the switch

IPv4 INTERFACE

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

Table 195: IPv4 Interface Commands

Command Group	Function
Basic IPv4 Configuration	Configures the IP address for interfaces and the gateway router
ARP Configuration	Configures static, dynamic and proxy ARP service

BASIC IPv4 CONFIGURATION This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 196: Basic IP Configuration Commands

Command	Function	Mode
<code>ip address</code>	Sets the IP address for the current interface	IC
<code>ip default-gateway</code>	Defines the default gateway through which this switch can reach other subnetworks	GC
<code>show ip interface</code>	Displays the IP settings for this device	PE
<code>show ip route</code>	Displays specified entries in the routing table	PE
<code>show ip traffic</code>	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
<code>traceroute</code>	Shows the route packets take to the specified host	PE
<code>ping</code>	Sends ICMP echo request packets to another node on the network	NE, PE

ip address This command sets the IPv4 address for the currently selected VLAN interface. Use the **no** form to restore the default 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.

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

DHCP

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that

network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.

- ◆ Before any network interfaces are configured on the router, first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- ◆ 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 be 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 router.



NOTE: Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router 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)#
```

RELATED COMMANDS

[ip dhcp restart client \(1359\)](#)
[ip default-gateway \(1370\)](#)
[ipv6 address \(1380\)](#)

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 from which the ping is sent.

EXAMPLE

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

RELATED COMMANDS

[ip address \(1368\)](#)
[ip route \(1408\)](#)
[ipv6 default-gateway \(1379\)](#)

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
  Proxy ARP is disabled
Console#
```

RELATED COMMANDS

[ip address \(1368\)](#)

[show ipv6 interface \(1388\)](#)

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 router 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 (see [page 1351](#)) and host name-to-address translation enabled (see [page 1348](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 1350](#)).

EXAMPLE

```

Console#ping 10.1.0.9
Type 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 \(974\)](#)

ARP CONFIGURATION This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 197: Address Resolution Protocol Commands

Command	Function	Mode
arp	Adds a static entry in the ARP cache	GC
arp timeout	Sets the time a dynamic entry remains in the ARP cache	GC
ip proxy-arp	Enables proxy ARP service	IC
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE
show arp	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.
- ◆ You may need to enter a static entry in the cache 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 \(1377\)](#)

[show arp \(1377\)](#)

arp timeout This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default timeout.

SYNTAX

arp timeout *seconds*

no arp timeout

seconds - The time a dynamic entry remains in the ARP cache.
(Range: 300-86400; 86400 seconds is one day)

DEFAULT SETTING

1200 seconds (20 minutes)

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.
- ◆ The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

EXAMPLE

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp timeout 900
Console(config)#
```

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.
Are you sure to continue this operation (y/n)?y
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.

EXAMPLE

This example displays all entries in the ARP cache.

```

Console#show arp
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address      Type      Interface
-----
10.1.1.0.0      FF-FF-FF-FF-FF-FF other      VLAN1

```

```
10.1.0.254      00-00-AB-CD-00-00 other    VLAN1
10.1.0.255      FF-FF-FF-FF-FF-FF other    VLAN1
145.30.20.23    09-50-40-30-20-10 dynamic  VLAN3

Total entry : 4
Console#
```

IPv6 INTERFACE

This switch supports the following IPv6 interface commands.

Table 198: 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	NE, PE
<code>show ipv6 interface</code>	Displays the usability and configured settings for IPv6 interfaces	NE, PE
<code>show ipv6 mtu</code>	Displays maximum transmission unit (MTU) information for IPv6 interfaces	NE, PE
<code>show ipv6 traffic</code>	Displays statistics about IPv6 traffic	NE, PE
<code>clear ipv6 traffic</code>	Resets IPv6 traffic counters	PE
<code>ping6</code>	Sends IPv6 ICMP echo request packets to another node on the network	PE
<code>traceroute6</code>	Shows the route packets take to the specified host	PE
<i>Neighbor Discovery</i>		
<code>ipv6 hop-limit</code>	Configures the maximum number of hops used in router advertisements that are originated by this router	GC
<code>ipv6 nd dad attempts</code>	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC
<code>ipv6 nd ns-interval</code>	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC

Table 198: IPv6 Configuration Commands (Continued)

Command	Function	Mode
<code>ipv6 nd raguard</code>	Blocks incoming Router Advertisement and Router Redirect packets	IC
<code>ipv6 nd reachable-time</code>	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred	IC
<code>clear ipv6 neighbors</code>	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE
<code>show ipv6 nd raguard</code>	Displays the configuration setting for RA Guard	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 from which the ping is sent.
- ◆ An IPv6 default gateway must be defined if the destination has been assigned an IPv6 address and 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 \(1388\)](#)

[ip default-gateway \(1370\)](#)

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 [ip 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::2E0:CFE:FE00:FD/64
Global unicast address(es):
    2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
    FF02::1:FE00:72
    FF02::1:FE00:FD
    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

Console#

```

RELATED COMMANDS

[ipv6 address eui-64 \(1383\)](#)
[ipv6 address autoconfig \(1381\)](#)
[show ipv6 interface \(1388\)](#)
[ip address \(1368\)](#)

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 2001:DB8:2222:7272:2E0:CFF:FE00:FD to the switch.

```
Console(config-if)#ipv6 address autoconfig
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
  2001:db8:2222:7272:2e0:cff:fe00:fd/64, subnet is 2001:db8:2222:7272::/
  64[AUTOCONFIG]
    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 \(1380\)](#)

[show ipv6 interface \(1388\)](#)

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::2E0:CFF:FE00:FD/64
Global unicast address(es):
    2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0/64[EUI]
    2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
    FF02::1:FF00:72
    FF02::1:FF00:FD
    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

Console#
```

RELATED COMMANDS

[ipv6 address autoconfig \(1381\)](#)
[show ipv6 interface \(1388\)](#)

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:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:2E0:CFE:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
  FF02::1:FF19:6779
  FF02::1:FF00:72
  FF02::1:FF00:FD

```

```
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
```

Console#

RELATED COMMANDS

[ipv6 enable \(1386\)](#)

[show ipv6 interface \(1388\)](#)

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 1383](#)). 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::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
  FF02::1:FF00:72
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1280 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

Console#

```

RELATED COMMANDS[ipv6 address link-local \(1385\)](#)[show ipv6 interface \(1388\)](#)

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 \(1390\)](#)
[jumbo frame \(733\)](#)

show ipv6 default-gateway

This command displays the current IPv6 default gateway.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following shows the default gateway configured for this device:

```
Console#show ipv6 default-gateway
IPv6 default gateway 2001:DB8:2222:7272::254

Console#
```

show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

SYNTAX

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix/prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

vlan-id - VLAN ID (Range: 1-4093)

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

COMMAND MODE

Normal Exec, 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::2E0:CFF:FE00:FD/64
Global unicast address(es):
    2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
    FF02::1:FF00:72
    FF02::1:FF00:FD
    FF02::1
IPv6 link MTU is 1280 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

Console#

```

Table 199: show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked "up" if the switch can send and receive packets on this interface, "down" if a line signal is not present, or "administratively down" if the interface has been disabled by the administrator.
IPv6	IPv6 is marked "enable" if the switch can send and receive IP traffic on this interface, "disable" if the switch cannot send and receive IP traffic on this interface, or "stalled" if a duplicate link-local address is detected on the interface.
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface
Joined group address(es)	<p>In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively.</p> <p>FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.</p> <p>A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.</p>
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.

Table 199: show ipv6 interface - display description (Continued)

Field	Description
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.

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 \(1371\)](#)

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 200: 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

Normal Exec, 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
    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
    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
multicast listener discovery version 2 reports

ICMPv6 sent
output
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
multicast listener discovery version 2 reports

UDP Statistics:
input
no port errors
other errors
output

Console#

```

Table 201: show ipv6 traffic - display description

Field	Description
<i>IPv6 Statistics</i>	
<i>IPv6 received</i>	
total received	The total number of input datagrams received by the interface, including those received in error.
header errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
too big errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
address errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
truncated packets	The number of input datagrams discarded because datagram frame didn't carry enough data.

Table 201: show ipv6 traffic - display description (Continued)

Field	Description
discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
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 ipv6IfStatsOutForwDatagrams.
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 ipv6IfStatsOutForwDatagrams 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 ipv6IfIcmpInErrors. 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.

Table 201: show ipv6 traffic - display description (Continued)

Field	Description
errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
destination unreachable messages	The number of ICMP Destination Unreachable messages received by the interface.
packet too big messages	The number of ICMP Packet Too Big messages received by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages received by the interface.
parameter problem message	The number of ICMP Parameter Problem messages received by the interface.
echo request messages	The number of ICMP Echo (request) messages received by the interface.
echo reply messages	The number of ICMP Echo Reply messages received by the interface.
router solicit messages	The number of ICMP Router Solicit messages received by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages received by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages received by the interface.
neighbor advertisement messages	The number of ICMP Neighbor Advertisement messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
group membership query messages	The number of ICMPv6 Group Membership Query messages received by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages received by the interface.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
multicast listener discovery version 2 reports	The number of MLDv2 reports received by the interface.
<i>ICMPv6 sent</i>	
output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by 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.

Table 201: show ipv6 traffic - display description (Continued)

Field	Description
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: 48-18024 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: 100 bytes

COMMAND MODE

Privileged Exec

COMMAND USAGE

- ◆ Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ When pinging a host name, be sure the DNS server has been enabled (see [page 1348](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 1350](#)).
- ◆ When using ping6 with a host name, the router 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%1/64
Type 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** *max-failures*]

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.

max-failures - The maximum number of failures before which the trace route is terminated. (Range: 1-255)

DEFAULT SETTING

Maximum failures: 5

COMMAND MODE

Privileged Exec

COMMAND USAGE

- ◆ Use the **traceroute6** command to determine the path taken to reach a specified destination.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off

before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

EXAMPLE

```
Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1/64
Press "ESC" to abort.

Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3
seconds, 5 max failure(s) before termination.

Hop  Packet 1 Packet 2 Packet 3 IPv6 Address
-----
  1    <10 ms   <10 ms   <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.
Console#
```

Neighbor Discovery

ipv6 hop-limit This command configures the maximum number of hops used in router advertisements that are originated by this router. Use the **no** form to restore the default setting.

SYNTAX

ipv6 hop-limit *hops*

no ipv6 hop-limit

hops - The maximum number of hops in router advertisements and all IPv6 packets. (Range: 1-255)

DEFAULT SETTING

1

COMMAND MODE

Interface Configuration (VLAN)

EXAMPLE

The following sets the hop limit for router advertisements to 64:

```
Console(config-if)#interface vlan 1
Console(config)#ipv6 hop-limit 64
Console(config)#
```

ipv6 nd dad attempts This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

DEFAULT SETTING

3

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ Configuring a value of 0 disables duplicate address detection.
- ◆ Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- ◆ Duplicate address detection is stopped on any interface that has been suspended (see the [vlan](#) command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- ◆ An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- ◆ If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
- ◆ If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

EXAMPLE

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The [show ipv6 interface](#) command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

RELATED COMMANDS

[ipv6 nd ns-interval \(1400\)](#)
[show ipv6 neighbors \(1404\)](#)

ipv6 nd ns-interval This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

DEFAULT SETTING

1000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.

- ◆ This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.
- ◆ Setting the neighbor solicitation interval to 0 means that the configured time is unspecified by this router.

EXAMPLE

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```

Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    FE80::200:E8FF:FE90:0/64
Global unicast address(es):
    2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
    FF01::1/16
    FF02::1/16
    FF02::1:FF00:79/104
    FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#

```

RELATED COMMANDS

[show running-config \(727\)](#)

ipv6 nd raguard This command blocks incoming Router Advertisement and Router Redirect packets. Use the no form to disable this feature.

SYNTAX

[no] ipv6 nd raguard

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- ◆ IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.
- ◆ This command can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 nd raguard
Console(config-if)#
```

ipv6 nd reachable-time

This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

SYNTAX

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability.
(Range: 0-3600000)

DEFAULT SETTING

30000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ The time limit configured by this command allows the router to detect unavailable neighbors.
- ◆ This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.
- ◆ Setting the time limit to 0 means that the configured time is unspecified by this router.

EXAMPLE

The following sets the reachable time for a remote node to 1000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#pv6 nd reachable-time 1000
Console(config)#
```

clear ipv6 neighbors This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

COMMAND MODE

Privileged Exec

EXAMPLE

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

show ipv6 nd raguard This command displays the configuration setting for RA Guard.

SYNTAX

show ipv6 nd raguard [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 nd raguard interface ethernet 1/1
Interface RA Guard
-----
Eth 1/ 1  Yes
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: 1-4093)

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 VLAN
FE80::2E0:CFF:FE9C:CA10 4       00-E0-0C-9C-CA-10 R      1
Console#
```

Table 202: 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.

Table 202: show ipv6 neighbors - display description (Continued)

Field	Description
State	<p>The following states are used for dynamic entries:</p> <p>I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.</p> <p>I2 (Invalid) - An invalidated mapping. Setting the state to invalid disassociates the interface identified with this entry from the indicated mapping (RFC 4293).</p> <p>R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.</p> <p>S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.</p> <p>D (Delay) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.</p> <p>P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.</p> <p>U (Unknown) - Unknown state.</p> <p>The following states are used for static entries:</p> <p>I1 (Incomplete)-The interface for this entry is down.</p> <p>R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.</p> <p>P2 (Permanent) - Indicates a static entry.</p>
VLAN	VLAN interface from which the address was reached.

RELATED COMMANDS[show mac-address-table \(1055\)](#)

After network interfaces are configured for the switch, the paths used to send traffic between different interfaces must be set. If routing is enabled on the switch, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Table 1: IP Routing Commands

Command Group	Function
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table and statistics for protocols used to exchange routing information
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP

GLOBAL ROUTING CONFIGURATION

Table 2: Global Routing Configuration Commands

Command	Function	Mode
ip route	Configures static routes	GC
show ip route	Displays specified entries in the routing table	PE
show ip route database	Displays static or dynamically learned entries in the routing table	PE
show ip route summary	Displays summary information for the routing table	PE
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE

IPv4 Commands

ip route This command configures static routes. Use the **no** form to remove static routes.

SYNTAX

ip route *destination-ip netmask next-hop [distance]*

no ip route {*destination-ip netmask next-hop* | *}

destination-ip – IP address of the destination network, subnetwork, or host.

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

next-hop – IP address of the next hop router used for this route.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 120 for RIP. (Range: 1-255, Default: 1)

* – Removes all static routing table entries.

DEFAULT SETTING

No static routes are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ Up to 512 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.
- ◆ If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- ◆ Static routes are included in RIP updates periodically sent by the router if this feature is enabled by the RIP **redistribute** command (see [page 1418](#)).

EXAMPLE

This example forwards all traffic for subnet 192.168.1.0 to the gateway router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

show ip route This command displays information in the Forwarding Information Base (FIB).

SYNTAX

show ip route [**connected** | **database** | **rip** | **static** | **summary**]

connected – Displays all currently connected entries.

database – All known routes, including inactive routes.

rip – Displays all entries learned through the Routing Information Protocol (RIP).

static – Displays all static entries.

summary – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- ◆ The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- ◆ This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the [show ip route database](#) command.

EXAMPLE

In the following example, note that the entry for RIP displays both the distance and metric for this route.

```
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

R      10.1.1.0/24 [120/2] via 192.168.1.10, VLAN1, 00:00:14
C      127.0.0.0/8 is directly connected, lo
C      192.168.1.0/24 is directly connected, VLAN1
Console#
```

show ip route database This command displays entries in the Routing Information Base (RIB).

COMMAND MODE

Privileged Exec

COMMAND USAGE

The RIB contains all available routes learned through dynamic routing protocols, 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).

EXAMPLE

```
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#
```

show ip route summary This command displays summary information for the routing table.

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, the numeric identifier following the named routing table (that is, the Forwarding Information Base) is the FIB ID.

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Connected          2
Total              2
Console#
```

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
    4877 total received
        header errors
        unknown protocols
        address errors
        discards
    4763 delivers
        reassembly request datagrams
        reassembled succeeded
        reassembled failed
IP sent
    forwards datagrams
    5927 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:
    2 input
        no port errors
        other errors
        output
TCP Statistics:
    4698 input
  
```

input errors
5867 output

Console#

ROUTING INFORMATION PROTOCOL (RIP)

Table 3: Routing Information Protocol Commands

Command	Function	Mode
<code>router rip</code>	Enables the RIP routing protocol	GC
<code>default-information originate</code>	Generates a default external route into an autonomous system	RC
<code>default-metric</code>	Sets the default metric assigned to external routes imported from other protocols	RC
<code>distance</code>	Defines an administrative distance for external routes learned from other routing protocols	RC
<code>maximum-prefix</code>	Sets the maximum number of RIP routes allowed	RC
<code>neighbor</code>	Defines a neighboring router with which to exchange information	RC
<code>network</code>	Specifies the network interfaces that are to use RIP routing	RC
<code>passive-interface</code>	Stops RIP from sending routing updates on the specified interface	RC
<code>redistribute</code>	Redistribute routes from one routing domain to another	RC
<code>timers basic</code>	Sets basic timers, including update, timeout, garbage collection	RC
<code>version</code>	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC
<code>ip rip authentication mode</code>	Specifies the type of authentication used for RIP2 packets	IC
<code>ip rip authentication string</code>	Enables authentication for RIP2 packets and specifies keys	IC
<code>ip rip receive version</code>	Sets the RIP receive version to use on a network interface	IC
<code>ip rip receive-packet</code>	Configures the interface to receive of RIP packets	IC
<code>ip rip send version</code>	Sets the RIP send version to use on a network interface	IC
<code>ip rip send-packet</code>	Configures the interface to send RIP packets	IC
<code>ip rip split-horizon</code>	Enables split-horizon or poison-reverse loop prevention	IC
<code>clear ip rip route</code>	Clears specified data from the RIP routing table	PE
<code>show ip protocols rip</code>	Displays RIP process parameters	PE
<code>show ip rip</code>	Displays information about RIP routes and configuration settings	PE

router rip This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

SYNTAX

[no] router rip

COMMAND MODE

Global Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ RIP is used to specify how routers exchange routing table information.
- ◆ This command is also used to enter router configuration mode.

EXAMPLE

```
Console(config)#router rip
Console(config-router)#
```

RELATED COMMANDS

[network \(1417\)](#)

default-information originate This command generates a default external route into the local RIP autonomous system. Use the **no** form to disable this feature.

SYNTAX

[no] default-information originate

DEFAULT SETTING

Disabled

COMMAND MODE

Router Configuration

COMMAND USAGE

This command sets a default route for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

EXAMPLE

```
Console(config-router)#default-information originate
Console(config-router)#
```

RELATED COMMANDS

[ip route \(1408\)](#)
[redistribute \(1418\)](#)

default-metric This command sets the default metric assigned to external routes imported from other protocols. Use the **no** form to restore the default value.

SYNTAX

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to external routes. (Range: 1-15)

DEFAULT SETTING

1

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ This command does not override the metric value set by the [redistribute](#) command. When a metric value has not been configured by the [redistribute](#) command, the **default-metric** command sets the metric value to be used for all imported external routes.
- ◆ The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- ◆ It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

EXAMPLE

This example sets the default metric to 5.

```
Console(config-router)#default-metric 5
Console(config-router)#
```

RELATED COMMANDS

[redistribute \(1418\)](#)

distance This command defines an administrative distance for external routes learned from other routing protocols. Use the **no** form to restore the default setting.

SYNTAX

[no] distance *distance network-address netmask [acl-name]*

distance - Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table.
(Range: 1-255)

network-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
(Range: 1-16 characters)

DEFAULT SETTING

None

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.
- ◆ An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.
- ◆ The administrative distance is applied to all routes learned for the specified network.

EXAMPLE

```
Console(config-router)#distance 2 192.168.3.0 255.255.255.0
Console(config-router)#
```

maximum-prefix This command sets the maximum number of RIP routes allowed by the system. Use the **no** form to restore the default setting.

SYNTAX

maximum-prefix *maximum-routes*

no maximum-prefix

maximum-routes - The maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168)

DEFAULT SETTING

1024

COMMAND MODE

Router Configuration

COMMAND USAGE

All the learned RIP routes may not be copied to the hardware tables in ASIC for fast data forwarding because of hardware resource limitations.

EXAMPLE

```
Console(config-router)#maximum-prefix 1024
Console(config-router)#
```

neighbor This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

SYNTAX

[no] neighbor *ip-address*

ip-address - IP address of a neighboring router.

DEFAULT SETTING

No neighbors are defined.

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ This command can be used to configure a static neighbor (specifically for point-to-point links) with which this router will exchange routing information, rather than relying on broadcast or multicast messages generated by the RIP protocol.
- ◆ Use this command in conjunction with the [passive-interface](#) command to control the routing updates sent to specific neighbors.

EXAMPLE

```
Console(config-router)#neighbor 10.2.0.254  
Console(config-router)#
```

RELATED COMMANDS

[passive-interface \(1418\)](#)

network This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

SYNTAX

[no] network {*ip-address netmask* | **vlan** *vlan-id*}

ip-address - IP address of a network directly connected to this router.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

vlan-id - VLAN ID. (Range: 1-4093)

DEFAULT SETTING

No networks are specified.

COMMAND MODE

Router Configuration

COMMAND USAGE

RIP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.

EXAMPLE

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0  
Console(config-router)#
```

RELATED COMMANDS

[router rip \(1413\)](#)

passive-interface This command stops RIP from sending routing updates on the specified interface. Use the **no** form to disable this feature.

SYNTAX

[**no**] **passive-interface** **vlan** *vlan-id*
vlan-id - VLAN ID. (Range: 1-4093)

DEFAULT SETTING

Disabled

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ If this command is used to stop sending routing updates on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on that interface will continue to be received and processed.
- ◆ Use this command in conjunction with the [neighbor](#) command to control the routing updates sent to specific neighbors.

EXAMPLE

```
Console(config-router)#passive-interface vlan1  
Console(config-router)#
```

RELATED COMMANDS

[neighbor \(1416\)](#)

redistribute This command imports external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into the autonomous system. Use the **no** form to disable this feature.

SYNTAX

[**no**] **redistribute** (**connected** | **ospf** | **static**) [**metric** *metric-value*]
connected - Imports routes that are established automatically just by enabling IP on an interface.
ospf - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.
static - Static routes will be imported into this routing domain.
metric-value - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

DEFAULT SETTING

redistribution - none

metric-value - set by the [default-metric](#) command

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ When a metric value has not been configured by the **redistribute** command, the **default-metric** command sets the metric value to be used for all imported external routes.
- ◆ A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- ◆ It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

EXAMPLE

This example redistributes routes learned from OSPF and sets the metric for all external routes imported from OSPF to a value of 3.

```
Console(config-router)#redistribute ospf metric 3
Console(config-router)#
```

This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

RELATED COMMANDS

[default-metric \(1414\)](#)

timers basic This command configures the RIP update timer, timeout timer, and garbage- collection timer. Use the **no** form to restore the defaults.

SYNTAX

timers basic *update timeout garbage*

no timers basic

update – Sets the update timer to the specified value.
(Range: 5-2147483647 seconds)

timeout – Sets the timeout timer to the specified value.
(Range: 90-360 seconds)

garbage – Sets the garbage collection timer to the specified value.
(Range: 60-240 seconds)

DEFAULT SETTING

Update: 30 seconds

Timeout: 180 seconds

Garbage collection: 120 seconds

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- ◆ The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- ◆ After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to it being purged by this device.
- ◆ Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- ◆ These timers must be set to the same values for all routers in the network.

EXAMPLE

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```


version This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

SYNTAX

version {1 | 2}

no version

1 - RIP Version 1

2 - RIP Version 2

DEFAULT SETTING

Receive: Accepts RIPv1 or RIPv2 packets

Send: Route information is broadcast to other routers with RIPv2.

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ When this command is used to specify a global RIP version, any VLAN interface not previously set by the [ip rip receive version](#) or [ip rip send version](#) command will use the global RIP version setting.
- ◆ When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the [ip rip receive version](#) or [ip rip send version](#) command will be set to the default send or receive version.
- ◆ Any configured interface settings take precedence over the global settings.

EXAMPLE

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

RELATED COMMANDS

[ip rip receive version \(1423\)](#)

[ip rip send version \(1425\)](#)

ip rip authentication mode This command specifies the type of authentication that can be used for RIPv2 packets. Use the **no** form to restore the default value.

SYNTAX

ip rip authentication mode {md5 | text}

no ip rip authentication mode

md5 - Message Digest 5 (MD5) authentication

text - Indicates that a simple password will be used.

DEFAULT SETTING

Text authentication

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ The password to be used for authentication is specified in the [ip rip authentication string](#) command.
- ◆ This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- ◆ For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.
- ◆ MD5 is a one-way hash algorithm that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

EXAMPLE

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

RELATED COMMANDS

[ip rip authentication string \(1423\)](#)

ip rip authentication string This command specifies an authentication key for RIPv2 packets. Use the **no** form to delete the authentication key.

SYNTAX

ip rip authentication string *key-string*

no ip rip authentication string

key-string - A password used for authentication.
(Range: 1-16 characters, case sensitive)

DEFAULT SETTING

No authentication key

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- ◆ For authentication to function properly, both the sending and receiving interface must be configured with the same password, and authentication enabled by the [ip rip authentication mode](#) command.

EXAMPLE

This example sets an authentication password of "small" to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication string small
Console(config-if)#
```

RELATED COMMANDS

[ip rip authentication mode \(1422\)](#)

ip rip receive version This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

SYNTAX

ip rip receive version {1 | 2}

no ip rip receive version

- 1** - Accepts only RIPv1 packets.
- 2** - Accepts only RIPv2 packets.

DEFAULT SETTING

RIPv1 or RIPv2 packets

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ Use this command to override the global setting specified by the RIP [version](#) command.
- ◆ You can specify the receive version based on these options:
 - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use the default of version 1 or 2 if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

EXAMPLE

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

RELATED COMMANDS

[version \(1421\)](#)

ip rip receive-packet This command configures the interface to receive RIP packets. Use the **no** form to disable this feature.

SYNTAX

[no] ip rip receive-packet

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

Enabled

COMMAND USAGE

Use the **no** form of this command if it is not required to add any dynamic entries to the routing table for an interface. For example, when only static routes are to be allowed for a specific interface.

EXAMPLE

```

Console(config)#interface vlan 1
Console(config-if)#ip rip receive-packet
Console(config-if)#

```

RELATED COMMANDS

[ip rip send-packet \(1426\)](#)

ip rip send version This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

SYNTAX

ip rip send version {1 | 2 | 1-compatible}

no ip rip send version

1 - Sends only RIPv1 packets.

2 - Sends only RIPv2 packets.

1-compatible - Route information is broadcast to other routers with RIPv2.

DEFAULT SETTING

1-compatible (Route information is broadcast to other routers with RIPv2)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ Use this command to override the global setting specified by the [RIP version](#) command.
- ◆ You can specify the send version based on these options:
 - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use "1-compatible" to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information.)

EXAMPLE

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```

Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#

```

RELATED COMMANDS

[version \(1421\)](#)

ip rip send-packet This command configures the interface to send RIP packets. Use the **no** form to disable this feature.

[no] ip rip send-packet

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

Enabled

COMMAND USAGE

The **no** form of this command allows the router to passively monitor route information advertised by other routers attached to the network, without transmitting any RIP updates.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send-packet
Console(config-if)#
```

RELATED COMMANDS

[ip rip receive-packet \(1424\)](#)

ip rip split-horizon This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable this function.

SYNTAX

ip rip split-horizon [poisoned]

no ip rip split-horizon

poisoned - Enables poison-reverse on the current interface.

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

split-horizon poisoned

COMMAND USAGE

- ◆ Split horizon never propagates routes back to an interface from which they have been acquired.
- ◆ Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)
- ◆ If split-horizon is disabled with the **no rip ip split-horizon** command, and a loop occurs, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

EXAMPLE

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

clear ip rip route This command clears specified data from the RIP routing table.

SYNTAX

clear ip rip route {*ip-address netmask* | **all** | **connected** | **ospf** | **rip** | **static**}

ip-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

all - Deletes all entries from the routing table.

connected - Deletes all currently connected entries.

ospf - Deletes all entries learned through the Open Shortest Path First routing protocol.

rip - Deletes all entries learned through the Routing Information Protocol.

static - Deletes all static entries.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command with the "all" parameter clears the RIP table of all routes. To avoid deleting the entire RIP network, use the [redistribute connected](#) command to make the RIP network a connected route. To delete

the RIP routes learned from neighbors and also keep the RIP network intact, use the “rip” parameter with this command (**clear ip rip route rip**).

EXAMPLE

This example clears one specific route.

```
Console#clear ip rip route 192.168.1.0 255.255.255.0
Console#
```

show ip protocols This command displays RIP process parameters.
rip

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version by interface set, receive version by
  interface set
    Interface  Send          Recv
    VLAN1      1-compatible 1 2
  Routing for Networks:
    10.0.0.0/24
  Routing Information Sources:
    Gateway         Distance  Last Update  Bad Packets  Bad Routes
    10.0.0.2          120      00:00:13      0            0
  The maximum number of RIP routes allowed: 7872
  Distance: Default is 120
Console#
```

show ip rip This command displays information about RIP routes and configuration settings. Use this command without any keywords to display all RIP routes.

SYNTAX

show ip rip [interface [vlan *vlan-id*]]

interface - Shows RIP configuration settings for all interfaces or for a specified interface.

vlan-id - VLAN ID. (Range: 1-4093)

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       C - Connected, S - Static, O - OSPF

      Network          Next Hop      Metric From      Interface Time
Rc 192.168.0.0/24      1          1          VLAN1      01:57
Console#show ip rip interface vlan 1
Interface: vlan1
Routing Protocol: RIP
  Receive RIPv1 and RIPv2 packets
  Send RIPv1 Compatible
  Passive interface: Disabled
  Authentication mode: (None)
  Authentication string: (None)
  Split horizon: Enabled with Poisoned Reverse
  IP interface address: 192.168.0.2/24
Console#

```


SECTION IV

APPENDICES

This section provides additional information and includes these items:

- ◆ ["Software Specifications" on page 1433](#)
- ◆ ["Troubleshooting" on page 1437](#)
- ◆ ["License Information" on page 1439](#)

SOFTWARE FEATURES

MANAGEMENT AUTHENTICATION Local, RADIUS, TACACS+, Port Authentication (802.1X), HTTPS, SSH, Port Security, IP Filter

GENERAL SECURITY MEASURES Access Control Lists (512 rules), Port Authentication (802.1X), MAC Authentication, Port Security, DHCP Snooping, IP Source Guard

PORT CONFIGURATION 1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex
1000BASE-SX/LX/ZX: 1000 Mbps at full duplex (SFP³⁸, SFP+)
10GBASE-SR/LR/ER: 10 Gbps at full duplex (SFP+)

FLOW CONTROL Full Duplex: IEEE 802.3-2005
Half Duplex: Back pressure

STORM CONTROL Broadcast, multicast, or unknown unicast traffic throttled above a critical threshold

PORT MIRRORING 10 sessions, one or more source ports to one destination port

RATE LIMITS Input/Output Limits
Range configured per port

PORT TRUNKING Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

SPANNING TREE ALGORITHM Spanning Tree Protocol (STP, IEEE 802.1D-2004)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004)
Multiple Spanning Tree Protocol (MSTP, IEEE 802.1D-2004)

38. ECS4510-28F

VLAN SUPPORT Up to 4093 groups; port-based, protocol-based, tagged (802.1Q), voice VLANs, IP subnet, MAC-based, QinQ tunnel, GVRP for automatic VLAN learning

CLASS OF SERVICE Supports four levels of priority
Strict, Weighted Round Robin (WRR), or a combination of strict and weighted queueing
Layer 3/4 priority mapping: IP DSCP

QUALITY OF SERVICE DiffServ³⁹ supports class maps, policy maps, and service policies

MULTICAST FILTERING IGMP Snooping (Layer 2 IPv4)
Multicast VLAN Registration (IPv4/IPv6)

ADDITIONAL FEATURES BOOTP Client
Connectivity Fault Management
DHCP Client, Relay
DNS Client, Proxy
ERPS (Ethernet Ring Protection Switching)
LLDP (Link Layer Discover Protocol)
OAM (Operation, Administration, and Maintenance)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts
SNMP (Simple Network Management Protocol)
SNTP (Simple Network Time Protocol)

MANAGEMENT FEATURES

IN-BAND MANAGEMENT Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell

**OUT-OF-BAND
MANAGEMENT** RS-232 DB-9 console port

SOFTWARE LOADING HTTP, FTP or TFTP in-band, or XModem out-of-band

SNMP Management access via MIB database
Trap management to specified hosts

³⁹. Currently only supported for IPv4.

RMON Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

STANDARDS

Ethernet Service OAM (ITU-T Y.1731) - partial support
 IEEE 802.1AB Link Layer Discovery Protocol
 IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
 Spanning Tree Protocol
 Rapid Spanning Tree Protocol
 Multiple Spanning Tree Protocol
 IEEE 802.1p Priority tags
 IEEE 802.1Q VLAN
 IEEE 802.1v Protocol-based VLANs
 IEEE 802.1X Port Authentication
 IEEE 802.3-2005
 Ethernet, Fast Ethernet, Gigabit Ethernet
 Link Aggregation Control Protocol (LACP)
 Full-duplex flow control (ISO/IEC 8802-3)
 IEEE 802.3ac VLAN tagging
 IEEE 802.1ag Connectivity Fault Management (Amendment 5, D7.1)
 DHCP Client (RFC 2131)
 HTTPS
 ICMP (RFC 792)
 IGMP (RFC 1112)
 IGMPv2 (RFC 2236)
 IGMPv3 (RFC 3376) - partial support
 IPv4 IGMP (RFC 3228)
 RADIUS+ (RFC 2618)
 RMON (RFC 2819 groups 1,2,3,9)
 SNMP (RFC 1157)
 SNMPv2c (RFC 1901, 2571)
 SNMPv3 (RFC DRAFT 2273, 2576, 3410, 3411, 3413, 3414, 3415)
 SNTP (RFC 2030)
 SSH (Version 2.0)
 TELNET (RFC 854, 855, 856)
 TFTP (RFC 1350)

MANAGEMENT INFORMATION BASES

Bridge MIB (RFC 1493)
 Differentiated Services MIB (RFC 3289)
 DNS Resolver MIB (RFC 1612)

ERPS MIB (ITU-T G.8032)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
IPV6-MIB (RFC 2065)
IPV6-ICMP-MIB (RFC 2066)
IPV6-TCP-MIB (RFC 2052)
IPV6-UDP-MIB (RFC2054)
Link Aggregation MIB (IEEE 802.3ad)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
NTP (RFC 1305)
P-Bridge MIB (RFC 2674P)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Power Ethernet MIB (RFC 3621)
Private MIB
Q-Bridge MIB (RFC 2674Q)
QinQ Tunneling (IEEE 802.1ad Provider Bridges)
Quality of Service MIB
RADIUS Accounting Server MIB (RFC 2621)
RADIUS Authentication Client MIB (RFC 2619)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMP Community MIB (RFC 3584)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMPv2 IP MIB (RFC 2011)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 4: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	<ul style="list-style-type: none"> ◆ Be sure the switch is powered on. ◆ Check network cabling between the management station and the switch. Make sure the ends are properly connected and there is no damage to the cable. Test the cable if necessary. ◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. ◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	<ul style="list-style-type: none"> ◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. ◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. ◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service. Try using another SSH client or check for updates to your SSH client application. ◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. ◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none"> ◆ Check to see if you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 115200 bps. ◆ Verify that you are using the DB-9 null-modem serial cable supplied with the switch. If you use any other cable, be sure that it conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	<ul style="list-style-type: none"> ◆ Contact your local distributor.

USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the "show tech-support" command to record all system settings in this file.
9. Contact your distributor's service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
:
```

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

THE GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license

practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GLOSSARY

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP 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.

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 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 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.

**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.
- RMON** Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.
- RSTP** Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.
- SMTP** Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.
- SNMP** Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.
- SNTP** Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

- SSH** Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.
- STA** Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.
- TACACS+** Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.
- TCP/IP** Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.
- TELNET** Defines a remote communication facility for interfacing to a terminal device over TCP/IP.
- TFTP** Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.
- UDP** User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.
- UTC** Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.
- VLAN** Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.
- XMODEM** A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

COMMAND LIST

A

aaa accounting commands 838
aaa accounting dot1x 839
aaa accounting exec 840
aaa accounting update 841
aaa authorization exec 842
aaa group server 843
absolute 777
access-list arp 967
access-list ip 950
access-list ipv6 956
access-list mac 962
accounting commands 844
accounting dot1x 844
accounting exec 845
alias 975
arp 1375
arp timeout 1376
authentication enable 828
authentication login 829
authorization exec 845
auto-traffic-control 1029
auto-traffic-control action 1030
auto-traffic-control alarm-clear-threshold 1031
auto-traffic-control alarm-fire-threshold 1032
auto-traffic-control apply-timer 1028
auto-traffic-control auto-control-release 1033
auto-traffic-control control-release 1033
auto-traffic-control release-timer 1028

B

banner configure 717
banner configure company 718
banner configure dc-power-info 719
banner configure department 719
banner configure equipment-info 720
banner configure equipment-location 721
banner configure ip-lan 721
banner configure ip-number 722
banner configure manager-info 723
banner configure mux 723
banner configure note 724
boot system 735
bridge-ext gvrp 1120

C

calendar set 775
capabilities 975
channel-group 996
class 1186
class-map 1182
clear access-list hardware counters 970
clear arp-cache 1377
clear counters 982
clear dns cache 1352
clear efm oam counters 1341
clear erps statistics 1108
clear ethernet cfm ais mpid 1307
clear ethernet cfm errors 1319
clear ethernet cfm linktrace-cache 1328
clear ethernet cfm maintenance-points remote 1318
clear host 1353
clear ip dhcp snooping binding 920
clear ip dhcp snooping database flash 920
clear ip rip route 1427
clear ipv6 dhcp snooping binding 927
clear ipv6 dhcp snooping database flash 928
clear ipv6 neighbors 1403
clear ipv6 traffic 1395
clear log 760
clear mac-address-table dynamic 1055
clear network-access 903
clear pppoe intermediate-agent statistics 883
clock timezone 774
cluster 780
cluster commander 781
cluster ip-pool 781
cluster member 782
configure 711
control-vlan 1090
copy 736

D

databits 747
default-information originate 1413
default-metric 1414
delete 739
delete public-key 858

description 1183
 description 976
 dir 739
 disable 712
 disconnect 754
 distance 1415
 dos-protection echo-charge 943
 dos-protection smurf 944
 dos-protection tcp-flooding 944
 dos-protection tcp-null-scan 945
 dos-protection tcp-syn-fin-scan 945
 dos-protection tcp-xmas-scan 946
 dos-protection udp-flooding 946
 dos-protection win-nuke 947
 dot1q-tunnel system-tunnel-control 1136
 dot1x default 863
 dot1x eapol-pass-through 863
 dot1x identity profile 871
 dot1x intrusion-action 864
 dot1x max-reauth-req 865
 dot1x max-req 865
 dot1x max-start 871
 dot1x operation-mode 866
 dot1x pae supplicant 872
 dot1x port-control 867
 dot1x re-authenticate 870
 dot1x re-authentication 867
 dot1x system-auth-control 864
 dot1x timeout auth-period 873
 dot1x timeout held-period 873
 dot1x timeout quiet-period 868
 dot1x timeout re-authperiod 868
 dot1x timeout start-period 874
 dot1x timeout supp-timeout 869
 dot1x timeout tx-period 870

E

efm oam 1338
 efm oam critical-link-event 1338
 efm oam link-monitor frame 1339
 efm oam link-monitor frame threshold 1339
 efm oam link-monitor frame window 1340
 efm oam mode 1341
 efm oam remote-loopback 1342
 efm oam remote-loopback test 1343
 enable 1091
 enable 709
 enable password 824
 end 713
 erps 1089
 erps clear 1109
 erps domain 1089
 erps forced-switch 1109
 erps manual-switch 1111
 ethernet cfm ais level 1298

ethernet cfm ais ma 1299
 ethernet cfm ais period 1300
 ethernet cfm ais suppress alarm 1300
 ethernet cfm cc enable 1316
 ethernet cfm cc ma interval 1315
 ethernet cfm delay-measure two-way 1334
 ethernet cfm domain 1301
 ethernet cfm enable 1303
 ethernet cfm linktrace 1327
 ethernet cfm linktrace cache 1324
 ethernet cfm linktrace cache hold-time 1325
 ethernet cfm linktrace cache size 1326
 ethernet cfm loopback 1329
 ethernet cfm mep 1306
 ethernet cfm mep crosscheck 1323
 ethernet cfm mep crosscheck start-delay 1321
 ethernet cfm port-enable 1307
 exec-timeout 748
 exit 713

F

flowcontrol 977

G

garp timer 1121
 guard-timer 1092

H

holdoff-timer 1092
 hostname 716

I

interface 974
 interface vlan 1127
 ip access-group 954
 ip address 1368
 ip arp inspection 935
 ip arp inspection filter 936
 ip arp inspection limit 940
 ip arp inspection log-buffer logs 937
 ip arp inspection trust 940
 ip arp inspection validate 938
 ip arp inspection vlan 939
 ip default-gateway 1370
 ip dhcp client class-id 1358
 ip dhcp relay server 1364
 ip dhcp restart client 1359
 ip dhcp restart relay 1365
 ip dhcp snooping 912
 ip dhcp snooping database flash 921

ip dhcp snooping information option 914
 ip dhcp snooping information option circuit-id 918
 ip dhcp snooping information policy 915
 ip dhcp snooping trust 919
 ip dhcp snooping verify mac-address 916
 ip dhcp snooping vlan 917
 ip domain-list 1347
 ip domain-lookup 1348
 ip domain-name 1349
 ip host 1350
 ip http port 847
 ip http secure-port 848
 ip http secure-server 849
 ip http server 848
 ip igmp filter (Global Configuration) 1225
 ip igmp filter (Interface Configuration) 1228
 ip igmp max-groups 1228
 ip igmp max-groups action 1229
 ip igmp profile 1226
 ip igmp query-drop 1230
 ip igmp snooping 1203
 ip igmp snooping priority 1203
 ip igmp snooping proxy-reporting 1204
 ip igmp snooping querier 1205
 ip igmp snooping router-alert-option-check 1205
 ip igmp snooping router-port-expire-time 1206
 ip igmp snooping tcn-flood 1206
 ip igmp snooping tcn-query-solicit 1208
 ip igmp snooping unregistered-data-flood 1208
 ip igmp snooping unsolicited-report-interval 1209
 ip igmp snooping version 1210
 ip igmp snooping version-exclusive 1210
 ip igmp snooping vlan general-query-suppression 1211
 ip igmp snooping vlan immediate-leave 1212
 ip igmp snooping vlan last-memb-query-count 1213
 ip igmp snooping vlan last-memb-query-intvl 1213
 ip igmp snooping vlan mrd 1214
 ip igmp snooping vlan mrouters 1224
 ip igmp snooping vlan proxy-address 1215
 ip igmp snooping vlan query-interval 1216
 ip igmp snooping vlan query-resp-intvl 1217
 ip igmp snooping vlan static 1218
 ip name-server 1351
 ip proxy-arp 1376
 ip rip authentication mode 1422
 ip rip authentication string 1423
 ip rip receive version 1423
 ip rip receive-packet 1424
 ip rip send version 1425
 ip rip send-packet 1426
 ip rip split-horizon 1426
 ip route 1408
 ip source-guard 931
 ip source-guard binding 930
 ip source-guard max-binding 933
 ip ssh authentication-retries 855
 ip ssh crypto host-key generate 858
 ip ssh crypto zeroize 859
 ip ssh save host-key 860
 ip ssh server 856
 ip ssh server-key size 857
 ip ssh timeout 857
 ip telnet max-sessions 851
 ip telnet port 851
 ip telnet server 852
 ip tftp retry 744
 ip tftp timeout 745
 ipv6 access-group 961
 ipv6 address 1380
 ipv6 address autoconfig 1381
 ipv6 address eui-64 1383
 ipv6 address link-local 1385
 ipv6 default-gateway 1379
 ipv6 dhcp client rapid-commit vlan 1360
 ipv6 dhcp client rapid-commit vlan 1363
 ipv6 dhcp restart client vlan 1361
 ipv6 dhcp snooping 922
 ipv6 dhcp snooping max-binding 926
 ipv6 dhcp snooping trust 926
 ipv6 dhcp snooping vlan 925
 ipv6 enable 1386
 ipv6 hop-limit 1398
 ipv6 host 1352
 ipv6 mtu 1387
 ipv6 nd dad attempts 1399
 ipv6 nd ns-interval 1400
 ipv6 nd raguard 1401
 ipv6 nd reachable-time 1402

J

jumbo frame 733

L

l2protocol-tunnel tunnel-dmac 1142
 larp 996
 larp admin-key (Ethernet Interface) 998
 larp admin-key (Port Channel) 1000
 larp port-priority 999
 larp system-priority 1000
 larp timeout 1001
 line 747
 lldp 1271
 lldp admin-status 1275
 lldp basic-tlv management-ip-address 1275
 lldp basic-tlv port-description 1276
 lldp basic-tlv system-capabilities 1277
 lldp basic-tlv system-description 1277
 lldp basic-tlv system-name 1278
 lldp dot1-tlv proto-ident 1278
 lldp dot1-tlv proto-vid 1279
 lldp dot1-tlv pvid 1279
 lldp dot1-tlv vlan-name 1280
 lldp dot3-tlv link-aggr 1280
 lldp dot3-tlv mac-phy 1281
 lldp dot3-tlv max-frame 1281
 lldp dot3-tlv poe 1282
 lldp holdtime-multiplier 1271
 lldp med-fast-start-count 1272
 lldp med-location civic-addr 1282
 lldp med-notification 1284
 lldp med-tlv ext-poe 1285
 lldp med-tlv inventory 1285
 lldp med-tlv location 1286
 lldp med-tlv med-cap 1286
 lldp med-tlv network-policy 1287
 lldp notification 1287
 lldp notification-interval 1272
 lldp refresh-interval 1273
 lldp reinit-delay 1273
 lldp tx-delay 1274
 logging facility 757
 logging history 758
 logging host 759
 logging on 759
 logging sendmail 764
 logging sendmail destination-email 765
 logging sendmail host 764
 logging sendmail level 765
 logging sendmail source-email 766
 logging trap 760
 login 749
 loopback-detection 1042
 loopback-detection mode 1042
 loopback-detection recover-time 1043
 loopback-detection release 1044
 loopback-detection transmit-interval 1044

M

ma index name 1304
 ma index name-format 1305
 mac access-group 965
 mac-address-table aging-time 1053
 mac-address-table static 1054
 mac-authentication intrusion-action 902
 mac-authentication max-mac-count 902
 mac-authentication reauth-time 894
 mac-vlan 1159
 major-domain 1093
 management 877
 match 1184
 max-hops 1068
 maximum-prefix 1416
 media-type 978
 meg-level 1094
 memory 803
 mep archive-hold-time 1318
 mep crosscheck mpid 1322
 mep fault-notify alarm-time 1330
 mep fault-notify lowest-priority 1331
 mep fault-notify reset-time 1333
 mep-monitor 1094
 mst priority 1068
 mst vlan 1069
 mvr 1234
 mvr associated-profile 1234
 mvr domain 1235
 mvr immediate-leave 1241
 mvr priority 1237
 mvr profile 1235
 mvr proxy-query-interval 1236
 mvr proxy-switching 1237
 mvr robustness-value 1239
 mvr source-port-mode dynamic 1239
 mvr type 1242
 mvr upstream-source-ip 1240
 mvr vlan 1241
 mvr vlan group 1243
 mvr6 associated-profile 1253
 mvr6 domain 1253
 mvr6 immediate-leave 1259
 mvr6 profile 1254
 mvr6 proxy-query-interval 1255
 mvr6 proxy-switching 1255
 mvr6 robustness-value 1256
 mvr6 source-port-mode dynamic 1257
 mvr6 type 1260
 mvr6 upstream-source-ip 1258
 mvr6 vlan 1258
 mvr6 vlan group 1261

N

name 1070

negotiation 979
 neighbor 1416
 network 1417
 network-access aging 893
 network-access dynamic-qos 895
 network-access dynamic-vlan 896
 network-access guest-vlan 897
 network-access link-detection 897
 network-access link-detection link-down 898
 network-access link-detection link-up 898
 network-access link-detection link-up-down 899
 network-access mac-filter 893
 network-access max-mac-count 899
 network-access mode mac-authentication 900
 network-access port-mac-filter 901
 nlm 801
 no rspan session 1021
 node-id 1095
 non-erps-dev-protect 1096
 non-revertive 1097
 ntp authenticate 770
 ntp authentication-key 771
 ntp client 772
 ntp server 773

P

parity 750
 passive-interface 1418
 password 750
 password-thresh 751
 periodic 778
 permit, deny 1226
 permit, deny (ARP ACL) 968
 permit, deny (Extended IPv4 ACL) 952
 permit, deny (Extended IPv6 ACL) 958
 permit, deny (MAC ACL) 963
 permit, deny (Standard IP ACL) 951
 permit, deny (Standard IPv6 ACL) 957
 ping 1373
 ping6 1396
 police flow 1188
 police srtcm-color 1189
 police trtcm-color 1192
 policy-map 1186
 port channel load-balance 994
 port monitor 1013
 port security 888
 power inline 1007
 power inline maximum allocation 1008
 power inline priority 1009
 power-save 990
 pppoe intermediate-agent 879

pppoe intermediate-agent format-type 880
 pppoe intermediate-agent port-enable 881
 pppoe intermediate-agent port-format-type 881
 pppoe intermediate-agent trust 882
 pppoe intermediate-agent vendor-tag strip 883
 privilege 826
 process cpu 804
 prompt 707
 propagate-tc 1101
 protocol-vlan protocol-group (Configuring Groups) 1153
 protocol-vlan protocol-group (Configuring Interfaces) 1154

Q

qos map cos-dscp 1172
 qos map dscp-mutation 1174
 qos map phb-queue 1175
 qos map trust-mode 1176
 queue mode 1168
 queue weight 1169
 quit 710

R

radius-server acct-port 830
 radius-server auth-port 831
 radius-server host 831
 radius-server key 832
 radius-server retransmit 832
 radius-server timeout 833
 range 1227
 raps-def-mac 1102
 raps-without-vc 1102
 rate-limit 1023
 rcommand 783
 redistribute 1418
 reload (Global Configuration) 708
 reload (Privileged Exec) 712
 rename 1185
 revision 1070
 ring-port 1104
 rmon alarm 808
 rmon collection history 810
 rmon collection rmon1 811
 rmon event 809
 router rip 1413
 rpl neighbor 1105
 rpl owner 1106
 rspan destination 1019
 rspan remote vlan 1020
 rspan source 1018

S

server 843
 service-policy 1197
 set cos 1194
 set ip dscp 1195
 set phb 1196
 sflow 815
 sflow destination 816
 sflow max-datagram-size 817
 sflow max-header-size 817
 sflow owner 818
 sflow polling-interval 818
 sflow sample 819
 sflow source 819
 sflow timeout 820
 show access-group 970
 show access-list 970
 show access-list arp 969
 show access-list tcam-utilization 726
 show accounting 846
 show arp 1377
 show auto-traffic-control 1038
 show auto-traffic-control interface 1038
 show banner 725
 show bridge-ext 1123
 show cable-diagnostics 989
 show calendar 776
 show class-map 1197
 show cluster 783
 show cluster candidates 784
 show cluster members 784
 show dns 1353
 show dns cache 1354
 show dos-protection 947
 show dot1q-tunnel 1141
 show dot1x 874
 show efm oam counters interface 1344
 show efm oam event-log interface 1344
 show efm oam remote-loopback interface 1345
 show efm oam status interface 1345
 show efm oam status remote interface 1346
 show erps 1113
 show ethernet cfm configuration 1308
 show ethernet cfm errors 1320
 show ethernet cfm fault-notify-generator 1333
 show ethernet cfm linktrace-cache 1328
 show ethernet cfm ma 1310
 show ethernet cfm maintenance-points local 1311
 show ethernet cfm maintenance-points local detail mep 1312
 show ethernet cfm maintenance-points remote crosscheck 1324
 show ethernet cfm maintenance-points remote detail 1313
 show ethernet cfm md 1310
 show garp timer 1124
 show gvrp configuration 1124
 show history 710
 show hosts 1354
 show interfaces brief 983
 show interfaces counters 983
 show interfaces protocol-vlan protocol-group 1156
 show interfaces status 985
 show interfaces switchport 986
 show interfaces transceiver 987
 show ip access-group 955
 show ip access-list 955
 show ip arp inspection configuration 941
 show ip arp inspection interface 941
 show ip arp inspection log 942
 show ip arp inspection statistics 942
 show ip arp inspection vlan 942
 show ip dhcp snooping 921
 show ip dhcp snooping binding 922
 show ip igmp filter 1230
 show ip igmp profile 1231
 show ip igmp query-drop 1231
 show ip igmp snooping 1218
 show ip igmp snooping group 1220
 show ip igmp snooping mrouter 1221
 show ip igmp snooping statistics 1221
 show ip igmp throttle interface 1232
 show ip interface 1371
 show ip protocols rip 1428
 show ip rip 1428
 show ip route 1409
 show ip route database 1410
 show ip route summary 1410
 show ip source-guard 933
 show ip source-guard binding 934
 show ip ssh 860
 show ip telnet 852
 show ip tftp 745
 show ip traffic 1371
 show ip traffic 1411
 show ipv6 access-group 961
 show ipv6 access-list 960
 show ipv6 default-gateway 1388
 show ipv6 dhcp duid 1362
 show ipv6 dhcp snooping 928
 show ipv6 dhcp snooping binding 928
 show ipv6 dhcp snooping statistics 929
 show ipv6 dhcp vlan 1363
 show ipv6 interface 1388
 show ipv6 mtu 1390
 show ipv6 nd rguard 1403
 show ipv6 neighbors 1404

```

show ipv6 traffic 1391
show l2protocol-tunnel 1145
show lacp 1002
show line 756
show lldp config 1288
show lldp info local-device 1289
show lldp info remote-device 1290
show lldp info statistics 1293
show log 761
show logging 762
show logging sendmail 766
show loopback-detection 1044
show mac access-group 966
show mac access-list 966
show mac-address-table 1055
show mac-address-table aging-time 1056
show mac-address-table count 1057
show mac-vlan 1159
show management 878
show memory 726
show mvr 1244
show mvr associated-profile 1245
show mvr interface 1246
show mvr members 1247
show mvr profile 1249
show mvr statistics 1249
show mvr6 1262
show mvr6 associated-profile 1263
show mvr6 interface 1263
show mvr6 members 1264
show mvr6 profile 1265
show mvr6 statistics 1266
show network-access 903
show network-access mac-address-table 904
show network-access mac-filter 905
show nlm oper-status 803
show ntp 774
show policy-map 1198
show policy-map interface 1199
show port monitor 1015
show port security 890
show port-channel load-balance 1005
show power inline status 1010
show power mainpower 1011
show power-save 991
show pppoe intermediate-agent info 884
show pppoe intermediate-agent statistics 885
show privilege 827
show process cpu 727
show protocol-vlan protocol-group 1155
show public-key 860
show qos map cos-dscp 1177
show qos map dscp-mutation 1177
show qos map phb-queue 1178
show qos map trust-mode 1179
show queue mode 1171
show queue weight 1171
show radius-server 833
show reload 713
show rmon alarms 812
show rmon events 812
show rmon history 812
show rmon statistics 813
show rspan 1022
show running-config 727
show sflow 820
show snmp 789
show snmp engine-id 798
show snmp group 798
show snmp notify-filter 803
show snmp user 799
show snmp view 800
show snmp 770
show spanning-tree 1084
show spanning-tree mst configuration 1086
show ssh 861
show startup-config 729
show subnet-vlan 1158
show system 729
show tacacs-server 837
show tech-support 730
show time-range 779
show traffic-segmentation 1152
show udd 1050
show upgrade 744
show users 731
show version 732
show vlan 1134
show vlan-translation 1147
show voice vlan 1165
show watchdog 732
show web-auth 910
show web-auth interface 910
show web-auth summary 911
shutdown 979
silent-time 752
snmp-server 787
snmp-server community 787
snmp-server contact 788
snmp-server enable port-traps atc broadcast-alarm-clear 1034
snmp-server enable port-traps atc broadcast-alarm-fire 1034
snmp-server enable port-traps atc broadcast-control-apply 1035
snmp-server enable port-traps atc broadcast-control-release 1035
snmp-server enable port-traps atc multicast-alarm-clear 1036
snmp-server enable port-traps atc multicast-alarm-fire 1036

```

snmp-server enable port-traps atc
 multicast-control-apply 1037
 snmp-server enable port-traps atc
 multicast-control-release 1037
 snmp-server enable traps 790
 snmp-server enable traps ethernet cfm
 cc 1317
 snmp-server enable traps ethernet cfm
 crosscheck 1321
 snmp-server engine-id 793
 snmp-server group 794
 snmp-server host 791
 snmp-server location 788
 snmp-server notify-filter 801
 snmp-server user 795
 snmp-server view 797
 snmp client 768
 snmp poll 769
 snmp server 769
 spanning-tree 1060
 spanning-tree bpdu-filter 1071
 spanning-tree bpdu-guard 1072
 spanning-tree cisco-prestandard 1061
 spanning-tree cost 1073
 spanning-tree edge-port 1074
 spanning-tree forward-time 1061
 spanning-tree hello-time 1062
 spanning-tree link-type 1075
 spanning-tree loopback-detection
 1075
 spanning-tree loopback-detection
 action 1076
 spanning-tree loopback-detection
 release 1082
 spanning-tree loopback-detection
 release-mode 1077
 spanning-tree loopback-detection trap
 1078
 spanning-tree max-age 1063
 spanning-tree mode 1063
 spanning-tree mst configuration 1066
 spanning-tree mst cost 1078
 spanning-tree mst port-priority 1079
 spanning-tree pathcost method 1065
 spanning-tree port-bpdu-flooding
 1080
 spanning-tree port-priority 1080
 spanning-tree priority 1065
 spanning-tree protocol-migration 1083
 spanning-tree root-guard 1081
 spanning-tree spanning-disabled 1082
 spanning-tree system-bpdu-flooding
 1067
 spanning-tree transmission-limit 1067
 speed 752
 speed-duplex 980
 stopbits 753
 subnet-vlan 1157

switchport acceptable-frame-types
 1128
 switchport allowed vlan 1129
 switchport dot1q-tunnel mode 1137
 switchport dot1q-tunnel service match
 cvid 1138
 switchport dot1q-tunnel tpid 1140
 switchport forbidden vlan 1122
 switchport gvrp 1122
 switchport ingress-filtering 1130
 switchport l2protocol-tunnel 1144
 switchport mode 1131
 switchport native vlan 1131
 switchport packet-rate 981
 switchport priority default 1170
 switchport vlan-translation 1146
 switchport voice vlan 1163
 switchport voice vlan priority 1163
 switchport voice vlan rule 1164
 switchport voice vlan security 1165

T

tacacs-server host 834
 tacacs-server key 835
 tacacs-server port 836
 tacacs-server retransmit 836
 tacacs-server timeout 837
 terminal 755
 test cable-diagnostics 988
 timeout login response 754
 time-range 776
 timers basic 1420
 traceroute 1372
 traceroute6 1397
 traffic-segmentation 1148
 traffic-segmentation session 1150
 traffic-segmentation uplink/downlink
 1150
 traffic-segmentation uplink-to-uplink
 1151

U

udld aggressive 1048
 udld message-interval 1047
 udld port 1049
 upgrade opcode auto 741
 upgrade opcode path 742
 upgrade opcode reload 743
 username 825

V

version 1107
 version 1421
 vlan 1126
 vlan database 1125

vlan-trunking 1132
voice vlan 1160
voice vlan aging 1161
voice vlan mac-address 1162

W

watchdog software 732
web-auth 908

web-auth login-attempts 906
web-auth quiet-period 907
web-auth re-authenticate (IP) 909
web-auth re-authenticate (Port) 909
web-auth session-timeout 907
web-auth system-auth-control 908
whichboot 740
wtr-timer 1108

INDEX

NUMERICS

- 802.1Q tunnel 206, 1135
 - access 214, 1137
 - configuration, guidelines 210
 - configuration, limitations 209
 - CVID to SVID map 211, 1138
 - description 206
 - ethernet type 210, 1140
 - interface configuration 213, 1137–1140
 - mode selection 214, 1137
 - status, configuring 210, 1136
 - TPID 210, 1140
 - uplink 214, 1137
- 802.1X
 - authenticator, configuring 385, 864–870
 - global settings 384, 863–864
 - port authentication 382, 862, 864
 - port authentication accounting 313, 314, 844
 - supplicant, configuring 389, 871–874

A

- AAA
 - accounting 802.1X port settings 313, 314, 844
 - accounting exec command privileges 313, 840, 844
 - accounting exec settings 314, 845
 - accounting summary 315, 846
 - accounting update 313, 841
 - accounting, configuring 313, 838
 - authorization & accounting 306, 838
 - authorization exec settings 319, 842
 - authorization method 319, 842
 - authorization settings 319, 842
 - authorization summary 846
 - RADIUS group settings 314, 843
 - TACACS+ group settings 314, 843
- acceptable frame type 200, 1128
- Access Control List *See* ACL
- ACL 347, 949
 - ARP 353, 364, 967
 - binding to a port 366, 954
 - IPv4 Extended 353, 356, 949, 952
 - IPv4 Standard 353, 354, 949, 951
 - IPv6 Extended 353, 360, 956, 958
 - IPv6 Standard 353, 358, 956, 957
 - MAC 353, 362, 962
 - time range 349, 776
- Address Resolution Protocol *See* ARP

- address table 227, 1053
 - aging time 229, 1053
 - aging time, displaying 229, 1056
 - aging time, setting 229, 1053
- administrative users, displaying 731
- ARP
 - configuration 662
 - description 661
 - proxy 662, 1376
 - statistics 666, 1411
- ARP ACL 364, 936
- ARP configuration 1374
- ARP inspection 370, 934
 - ACL filter 373, 936
 - additional validation criteria 372, 938
 - ARP ACL 374, 967
 - enabling globally 372, 935
 - enabling per VLAN 374, 939
 - trusted ports 375, 940
- ARP statistics 1371
- ATC 263, 1025
 - control response 266, 1030
 - functional limitations 264, 1027
 - limiting traffic rates 263, 1026
 - shutting down a port 264, 1027
 - thresholds 266, 1031–1032
 - timers 264, 1028
 - usage 263, 1026
- authentication
 - MAC address authentication 326, 892, 900
 - MAC, configuring ports 330, 892
 - network access 326, 892, 900
 - public key 341, 854
 - web 324, 908
 - web authentication for ports, configuring 325, 908
 - web authentication port information, displaying 325, 910
 - web authentication, re-authenticating address 325, 909
 - web authentication, re-authenticating ports 325, 909
 - web, configuring 324, 908
- Automatic Traffic Control *See* ATC

B

- BOOTP 618, 1368
- BPDU 236
 - filter 249, 1071

- flooding when STA disabled on VLAN 241, 1080
- flooding when STA globally disabled 241, 1067
- ignoring superior BPDUs 248, 1081
- selecting protocol based on message format 249, 1083
- shut down port on receipt 249, 1072
- bridge extension capabilities, displaying 123, 1123
- broadcast storm, threshold 260, 261, 981

C

- cable diagnostics 166, 988

- canonical format indicator 280

CFM

- basic operations 512
- continuity check errors 545, 1319, 1320
- continuity check messages 501, 510, 512, 513, 1096, 1295, 1315, 1316
- cross-check errors 1317, 1321, 1323
- cross-check message 510, 513, 1295, 1321, 1323, 1324
- cross-check start delay 514, 1321
- delay measure 534, 1334
- description 510
- domain service access point 510, 522, 527, 1302
- fault isolation 510, 1295, 1327
- fault notification 510, 544, 1295, 1330, 1331, 1333
- fault notification generator 513, 519, 544, 1331, 1333
- fault verification 510, 1295
- link trace cache 543, 1325, 1326, 1328
- link trace message 510, 512, 530, 1295, 1324, 1325, 1327
- loop back messages 510, 512, 532, 1295, 1329
- maintenance association 510, 522, 1295, 1304, 1310
- maintenance domain 510, 511, 517, 1295, 1301, 1310
- maintenance end point 511, 513, 518, 523, 527, 536, 537, 1303, 1306, 1311
- maintenance intermediate point 511, 518, 539, 1301, 1302, 1304, 1311
- maintenance level 511, 512, 1301
- maintenance point 510, 1295, 1311
- MEP archive 520, 1318
- MEP direction 527, 1306
- remote maintenance end point 513, 522, 528, 537, 540, 541, 1312, 1313, 1318, 1322
- service instance 510, 512, 1304
- SNMP traps 515, 1317, 1321

class map

- description 1183
- DiffServ 284, 1182

- Class of Service See CoS

CLI

- command modes 698
- showing commands 696

- clustering switches, management access 481, 780

- command line interface See CLI

- committed burst size, QoS policy 291, 292, 293, 1188, 1189, 1192

- committed information rate, QoS policy 291, 292, 293, 1188, 1189, 1192

- community string 92, 456, 787

- configuration file, DHCP download reference 90

- configuration files, restoring defaults 125, 734

- configuration settings

- restoring 95, 127, 128, 734, 736

- saving 95, 127, 734, 736

- Connectivity Fault Management See CFM

- console port, required connections 80

- continuity check errors, CFM 545, 1319, 1320

- continuity check messages, CFM 501, 510, 512, 513, 1096, 1295, 1315, 1316

- CoS 269, 1176

- configuring 269, 1167

- default mapping to internal values 280, 1173

- enabling 276, 1176

- layer 3/4 priorities 276, 1172

- priorities, mapping to internal values 280, 1172

- queue mapping 273, 1175

- queue mode 270, 1168

- queue weights, assigning 272, 1169

- CoS/CFI to PHB/drop precedence 280, 1172

CPU

- status 145, 727

- utilization, setting trap 804

- utilization, showing 145, 727

- cross-check errors, CFM 1317, 1321, 1323

- cross-check message, CFM 510, 513, 1295, 1321, 1323, 1324

- cross-check start delay, CFM 514, 1321

- CVLAN to SPVLAN map 211, 1138

D

- default IPv4 gateway, configuration 1370

- default IPv6 gateway, configuration 621, 1379

- default priority, ingress port 269, 1170

- default settings, system 76

- delay measure, CFM 534, 1334

- DHCP 618, 645, 1368

- class identifier 646, 1358

- client 618, 1357, 1364, 1368

- client identifier 645, 646, 1358

- dynamic configuration 87

- option 82 information 404

- relay server 1364

- relay service 647

- relay service, enabling 648, 1365

- DHCPv4 snooping 402, 911

- circuit ID, setting 408, 918

- enabling 404, 912

- global configuration 404, 912

- information option 405, 914

- information option policy 405, 915

- information option, enabling 405, 914

- information option, remote ID 405, 914
- policy selection 405, 915
- specifying trusted interfaces 407, 919
- verifying MAC addresses 405, 916
- VLAN configuration 406, 917
- DHCPv6 snooping 922
 - enabling 922
 - global configuration 922
 - specifying trusted interfaces 926
 - VLAN configuration 925
- Differentiated Code Point Service *See* DSCP
- Differentiated Services *See* DiffServ
- DiffServ 283, 1181
 - binding policy to interface 297, 1197
 - class map 284, 1182, 1186
 - class map, description 1183
 - classifying QoS traffic 284, 1184
 - color aware, srTCM 292, 1189
 - color aware, trTCM 293, 1192
 - color blind, srTCM 292, 1189
 - color blind, trTCM 293, 1192
 - committed burst size 291, 292, 293, 1188, 1189, 1192
 - committed information rate 291, 292, 293, 1188, 1189, 1192
 - configuring 283, 1181
 - conforming traffic, configuring response 1188, 1189, 1192
 - description 1183
 - excess burst size 292, 1189
 - metering, configuring 287, 288, 289, 1188
 - peak burst size 293, 1192
 - peak information rate 293, 1192
 - policy map 287, 1186
 - policy map, description 285, 1183
 - QoS policy 287, 1186
 - service policy 297, 1197
 - setting CoS for matching packets 291, 1194
 - setting IP DSCP for matching packets 292, 293, 294, 1195
 - setting PHB for matching packets 291, 1196
 - single-rate, three-color meter 288, 292, 1189
 - srTCM metering 288, 292, 1189
 - traffic between CIR and BE, configuring response 292, 1189
 - traffic between CIR and PIR, configuring response 293, 1192
 - trTCM metering 293, 1192
 - two-rate, three-color meter 289, 1192
 - violating traffic, configuring response 294, 1188, 1189, 1192
- DNS
 - default domain name 639, 1349
 - displaying the cache 644, 1354
 - domain name list 639, 1350, 1352
 - enabling lookup 639, 1348
 - name server list 639, 1351
 - static entries, IPv4 643, 1350
 - static entries, IPv6 1352

- Domain Name Service *See* DNS
- domain service access point, CFM 510, 522, 527, 1302
- downloading software 125, 736
 - automatically 130, 741
 - using FTP or TFTP 130, 736
- drop precedence
 - CoS priority mapping 280, 1172
 - DSCP ingress map 278, 1174
- DSA encryption 344, 345, 858
- DSCP 276, 1176
 - enabling 276, 1176
 - ingress map, drop precedence 278, 1174
 - mapping to internal values 277, 1174
- DSCP to PHB/drop precedence 278, 1174
- dynamic addresses
 - clearing 231, 1055
 - displaying 230, 1055
- Dynamic Host Configuration Protocol *See* DHCP
- dynamic QoS assignment 327, 331, 895
- dynamic VLAN assignment 327, 331, 896

E

- edge port, STA 248, 251, 1074
- encryption
 - DSA 344, 345, 858
 - RSA 344, 345, 858
- engine ID 445, 446, 793
- ERPS
 - configuration guidelines 488, 1088
 - control VLAN 493, 1090
 - domain configuration 490, 1089
 - domain, enabling 492, 1091
 - global configuration 489, 1089
 - guard timer 502, 1092
 - hold-off timer 501, 1092
 - major domain 498, 1093
 - MEG level 493, 1094
 - node identifier 498, 1095
 - non-compliant device protection 1096
 - non-ERPS device protection 1096
 - propagate topology change 500, 1101
 - ring configuration 490, 1089
 - ring port, east interface 1104
 - ring port, west interface 1104
 - ring, enabling 492, 1091
 - RPL owner 1106
 - secondary ring 1093
 - status, displaying 505, 1113
 - wait-to-restore timer 502, 1108
 - WTR timer 502, 1108
- Ethernet Ring Protection Switching *See* ERPS
- event logging 412, 757
- excess burst size, QoS policy 292, 1192
- exec command privileges, accounting 313, 840, 844
- exec settings
 - accounting 314, 845
 - authorization 319, 842

F

fault isolation, CFM 510, 1295, 1327
 fault notification generator, CFM 513, 519, 544, 1331, 1333
 fault notification, CFM 510, 544, 1295, 1330, 1331, 1333
 fault verification, CFM 510, 1295
 FIB, description 1409
 firmware
 displaying version 121, 732
 upgrading 125, 736
 upgrading automatically 130, 741
 upgrading with FTP or TFTP 130, 741
 version, displaying 121, 732
 forwarding information base *See* FIB

G

GARP VLAN Registration Protocol *See* GVRP
 gateway, IPv4 default 1370
 gateway, IPv6 default 621, 1379
 general security measures 305, 887
 GVRP
 enabling 203, 1120
 global setting 203, 1120
 interface configuration 203, 1122

H

hardware version, displaying 121, 732
 HTTP, web server 848
 HTTPS 336, 338, 849
 configuring 336, 848, 849
 replacing SSL certificate 338, 736
 secure-site certificate 338, 736
 HTTPS, secure server 336, 849

I

IEEE 802.1D 235, 1063
 IEEE 802.1s 235, 1063
 IEEE 802.1w 235, 1063
 IEEE 802.1X 382, 862, 864
 IGMP
 filter profiles, configuration 580, 582, 1226
 filter, parameters 580, 582
 filtering & throttling 579, 1225
 filtering & throttling, configuring profile 1226, 1227
 filtering & throttling, creating profile 580, 1226
 filtering & throttling, enabling 579, 1225
 filtering & throttling, interface configuration 582, 1228–1229
 filtering & throttling, status 579, 1225
 groups, displaying 567, 1220
 Layer 2 558, 1201
 query 558, 560, 1205
 snooping 558, 1203
 snooping & query, parameters 560, 1201

 snooping, configuring 560, 1201
 snooping, immediate leave 569, 1212
 IGMP services, displaying 574, 1220
 IGMP snooping
 configuring 568, 1201
 enabling per interface 568, 569, 1203
 forwarding entries 574, 1220
 immediate leave, status 569, 1212
 interface attached to multicast router 565, 1221, 1224
 last leave 559
 last member query interval 571, 1213
 proxy address 572, 1215
 proxy reporting 570, 1204
 querier timeout 563, 1206
 query interval 571, 1216
 query response interval 571, 1217
 query suppression 559
 router port expire time 563, 1206
 static host interface 559, 1218
 static multicast routing 564, 1224
 static port assignment 566, 1218
 static router interface 559, 1224
 static router port, configuring 564, 1224
 statistics, displaying 575, 1221
 TCN flood 561, 1206
 unregistered data flooding 562, 1208
 version exclusive 562, 1210
 version for interface, setting 571, 1210
 version, setting 563, 1210
 with proxy reporting 559, 1204
 immediate leave, IGMP snooping 569, 1212
 importing user public keys 345, 736
 ingress filtering 200, 1130
 IP address
 BOOTP/DHCP 618
 setting 617
 IP address, setting 1367
 IP filter, for management access 378, 877
 IP routing 655, 671, 1407
 configuring interfaces 658
 unicast protocols 658, 1407
 IP source guard
 configuring static entries 399, 930
 setting filter criteria 397, 931
 setting maximum bindings 398, 933
 IP statistics 633, 1371, 1411
 IPv4 address
 BOOTP/DHCP 618, 1359, 1368
 dynamic configuration 87
 manual configuration 84
 setting 83, 617, 1368
 IPv6
 displaying neighbors 631, 1404
 duplicate address detection 631, 1399
 enabling 623, 1386
 hop-limit, advertisements 1398
 MTU 623, 1387
 neighbor reachable time 1402

- neighbor solicitation interval 1400
- router advertisements, blocking 626, 1401
- IPv6 address
 - dynamic configuration (global unicast) 88, 628, 1381
 - dynamic configuration (link-local) 88, 623, 1386
 - EUI format 628, 1383
 - EUI-64 setting 628, 1383
 - explicit configuration 623, 1386
 - global unicast 628, 1380
 - link-local 629, 1381
 - manual configuration (global unicast) 84, 628, 1380
 - manual configuration (link-local) 84, 629, 1385
 - setting 83, 621, 1380

J

- jumbo frame 122, 733

K

- key
 - private 340, 852
 - public 340, 852
 - user public, importing 345, 736
- key pair
 - host 340, 852
 - host, generating 344, 858

L

- LACP
 - configuration 172, 993
 - group attributes, configuring 176, 1000
 - group members, configuring 173, 996
 - local parameters 179, 1002
 - partner parameters 181, 1002
 - protocol message statistics 178, 1002
 - protocol parameters 173, 993
 - timeout, for LACPDU 173, 1001
- last member query interval, IGMP snooping 571, 1213
- layer 2, protocol tunnel 1144
- license information 1439
- Link Layer Discovery Protocol - Media Endpoint Discovery See LLDP-MED
- Link Layer Discovery Protocol See LLDP
- link trace cache, CFM 543, 1325, 1326, 1328
- link trace message, CFM 510, 512, 530, 1295, 1324, 1325, 1327
- link type, STA 248, 251, 1075
- LLDP 416, 1269
 - device statistics details, displaying 438, 1293
 - device statistics, displaying 436, 1293
 - display device information 424, 428, 1290
 - displaying remote information 428, 1290
 - interface attributes, configuring 419, 1275–1287

- local device information, displaying 424, 1289
- message attributes 419, 1269
- message statistics 436, 1293
- remote information, displaying 435, 436, 1290
- remote port information, displaying 428, 1290
- timing attributes, configuring 417, 1271–1274
- TLV 416, 419
 - TLV, 802.1 1278–1280
 - TLV, 802.3 1280–1282
 - TLV, basic 1275–1278
 - TLV, management address 419, 1275
 - TLV, port description 420, 1276
 - TLV, system capabilities 420, 1277
 - TLV, system description 420, 1277
 - TLV, system name 420, 1278
- LLDP-MED 417, 1269
 - notification, status 419, 1284
 - TLV 421, 1269
 - TLV, extended PoE 421, 1285
 - TLV, inventory 421, 1285
 - TLV, location 421, 1282, 1286
 - TLV, MED capabilities 421, 1286
 - TLV, network policy 421, 1287
 - TLV, PoE 421, 1285
- local engine ID 446, 793
- logging
 - messages, displaying 413, 761
 - syslog traps 414, 760
 - to syslog servers 414, 759
- log-in, web interface 100
- logon authentication 322, 823
 - encryption keys 310, 832, 835
 - RADIUS client 309, 830
 - RADIUS server 309, 830
 - sequence 307, 828, 829
 - settings 308, 310, 829
 - TACACS+ client 308, 834
 - TACACS+ server 308, 834
- logon banner, configuring 716
- loop back messages, CFM 510, 512, 532, 1295, 1329
- loopback detection
 - non-STA 1041
 - STA 238, 1075

M

- MAC address authentication 326, 892
 - ports, configuring 330, 892, 900
 - re-authentication 329
 - reauthentication 894
- MAC address, mirroring 232, 1013
- main menu, web interface 102
- maintenance association, CFM 510, 522, 1295, 1304, 1310
- maintenance domain, CFM 510, 511, 517, 1295, 1301, 1310
- maintenance end point, CFM 511, 513, 518, 523, 527, 536, 537, 1303, 1306, 1311

- maintenance intermediate point, CFM 511, 518, 539, 1301, 1302, 1304, 1311
- maintenance level, CFM 511, 512, 1301
- maintenance point, CFM 510, 1295, 1311
- management access, filtering per address 378, 877
- management access, IP filter 378, 877
- Management Information Bases (MIBs) 1435
- matching class settings, classifying QoS traffic 285, 1184
- media-type 152, 978
- memory
 - status 146, 726
 - utilization, showing 146, 726
- memory utilization, setting trap 803
- MEP archive, CFM 520, 1318
- mirror port
 - configuring 156, 1013
 - configuring local traffic 156, 1013
 - configuring remote traffic 158, 1016
- MSTP 253, 1063
 - global settings, configuring 240, 253, 1059
 - global settings, displaying 245, 1084
 - interface settings, configuring 246, 257, 1060, 1071–1082
 - interface settings, displaying 258, 1084
 - path cost 257, 1078
- MTU for IPv6 623, 1387
- multicast filtering 557, 1201
 - enabling IGMP snooping 569, 1203
 - enabling IGMP snooping per interface 568, 1203
 - router configuration 564, 1224
- multicast groups 567, 574, 1220
 - displaying 567, 574, 1220
 - static 566, 567, 1218, 1220
- multicast router discovery 568, 1214
- multicast router port, displaying 565, 1221
- multicast services
 - configuring 566, 1218
 - displaying 567, 1220
- multicast static router port 564, 1224
 - configuring 564, 1224
- multicast storm, threshold 261, 981
- Multicast VLAN Registration See MVR
- multicast, filtering and throttling 579, 1225
- MVR
 - assigning static multicast groups 594, 610, 1235, 1243
 - configuring 587, 1233, 1241
 - description 584
 - interface status, configuring 592, 1241–1243
 - interface status, displaying 593, 1244
 - IP for control packets sent upstream 588, 1240
 - proxy switching 585, 1237
 - receiver groups, displaying 596, 1247
 - robust value for proxy switching 586, 1239
 - setting interface type 593, 1242
 - setting multicast domain 587, 592, 1235
 - setting multicast groups 589, 1234, 1235
 - setting multicast priority 588, 1237

- specifying a domain 587, 592, 1235
- specifying a VLAN 587, 1234, 1241
- specifying priority 588, 1237
- static binding 594, 1235, 1243
- static binding, group to port 594, 1243
- statistics, displaying 597, 1249
- using immediate leave 593, 1241

MVR6

- assigning static multicast groups 610, 1254, 1261
- configuring 604, 1252, 1258
- interface status, configuring 608, 1259–1261
- interface status, displaying 609, 1264
- IP for control packets sent upstream 604, 1258
- proxy switching 602, 1255
- receiver groups, displaying 612, 1264
- robust value for proxy switching 602, 1256
- setting interface type 609, 1260
- setting multicast domain 609, 1253
- setting multicast groups 605, 1254
- specifying a domain 609, 1253
- specifying a VLAN 604, 1258
- static binding 610, 1254, 1261
- static binding, group to port 610, 1261
- statistics, displaying 613, 1266
- using immediate leave 609, 1259

N

network access

- authentication 326, 892
- dynamic QoS assignment 331, 895
- dynamic VLAN assignment 331, 896
- MAC address filter 331, 893
- port configuration 330, 900
- re-authentication 329
- reauthentication 894
- secure MAC information 335, 904, 905

NTP

- authentication keys, specifying 139, 771
- client, enabling 136, 772
- specifying servers 138, 773

NTP, setting the system clock 138, 770–774

O

OAM

- active mode 548, 1341
- displaying settings and status 547, 1344–1346
- enabling on switch ports 547, 1338
- errored frame link events 1339–1340
- event log, displaying 550, 1344
- message statistics, displaying 549, 1344
- mode selection 548, 1341
- passive mode 548, 1341
- remote device information, displaying 551, 1346
- remote loop back test 552, 1343
- setting to active mode 548, 1341

setting to passive mode 548, 1341
 Operations, Administration and Maintenance *See*
 OAM

P

password, line 750
 passwords 82, 322, 824
 administrator setting 322, 825
 path cost 251, 1073
 method 242, 1065
 STA 251, 1065, 1073
 peak burst size, QoS policy 293, 1192
 peak information rate, QoS policy 293, 1192
 per-hop behavior, DSCP ingress map 278, 1174
 policing traffic, QoS policy 287, 291
 policy map
 description 1183
 DiffServ 287, 1186
 port authentication 382, 862, 864
 port power
 displaying status 442, 1010
 inline 440, 1007
 inline status 442, 1010
 maximum allocation 440, 1008
 priority 441, 1009
 showing main power 442, 1011
 port priority
 configuring 269, 1167
 default ingress 269, 1170
 STA 247, 1080
 port security, configuring 380, 888
 port, statistics 162, 983
 ports
 autonegotiation 153, 979
 broadcast storm threshold 260, 261, 981
 capabilities 153, 975
 configuring 151, 973
 duplex mode 153, 980
 flow control 153, 977
 forced selection of media type 152, 978
 forced selection on combo ports 978
 mirroring 156, 1013
 mirroring local traffic 156, 1013
 mirroring remote traffic 158, 1016
 multicast storm threshold 261, 981
 speed 153, 980
 statistics 162, 983
 unknown unicast storm threshold 261, 981
 power budgets
 port 440, 1008
 port priority 441, 1009
 power savings
 configuring 182, 990
 enabling per port 182, 990
 PPPoE 648–653, 879–885
 priority, default port ingress 269, 1170
 private key 340, 852

privilege level, defining per command 826
 problems, troubleshooting 1437
 protocol migration 249, 1083
 protocol tunnel, layer 2 1144
 protocol VLANs 215, 1152
 configuring 215, 1153, 1154
 interface configuration 217, 1154
 system configuration 215, 1153
 proxy address, IGMP snooping 572, 1215
 proxy ARP 662, 1376
 proxy reporting, IGMP snooping 570, 1204
 public key 340, 852
 PVID, port native VLAN 199, 1131

Q

QinQ Tunneling *See* 802.1Q tunnel
 QoS 283, 1181
 configuration guidelines 1182
 configuring 283, 1181
 CoS/CFI to PHB/drop precedence 280, 1172
 DSCP to PHB/drop precedence 277, 1174
 dynamic assignment 331, 895
 matching class settings 285, 1184
 PHB to queue 273, 1175
 selecting DSCP, CoS 276, 1176
 QoS policy
 committed burst size 291, 292, 293, 1188, 1189,
 1192
 excess burst size 292, 1189
 peak burst size 293, 1192
 policing flow 287, 291
 srTCM 288, 1189
 srTCM police meter 292, 1189
 trTCM 289, 1192
 trTCM police meter 293, 1192
 QoS policy, committed information rate 291, 292,
 293, 1188, 1189, 1192
 QoS policy, peak information rate 293, 1192
 Quality of Service *See* QoS
 query interval, IGMP snooping 571, 1216
 query response interval, IGMP snooping 571, 1217
 queue weight, assigning to CoS 272, 1169

R

RADIUS
 logon authentication 309, 830
 settings 309, 830
 rate limit
 port 259, 1023
 setting 259, 1023
 remote engine ID 446, 793
 remote logging 414, 760
 remote maintenance end point, CFM 513, 522, 528,
 537, 540, 541, 1312, 1313, 1318, 1322
 Remote Monitoring *See* RMON
 rename, DiffServ 1185

restarting the system 147, 708, 712
 at scheduled times 147, 708
 showing restart time 150, 713

RIP 672, 1412
 authentication key 687, 1423
 authentication mode 687, 1422
 clearing routes 1427
 configuration settings, displaying 1428
 configuring 672, 1413–1428
 default external route 674, 1413
 default metric 674, 1414
 description 671
 global settings 673, 1413–1420
 interface protocol settings 685, 1417–1426
 interface, enabling 677, 1417
 neighbor router 680, 689, 1416
 passively monitoring updates 679, 1418
 poison reverse 672, 687, 1426
 process parameters, displaying 1428
 protocol packets, receiving 687, 1424
 protocol packets, sending 686, 1426
 receive version 686, 1423
 redistributing external routing information 681, 1418
 routes, clearing 1427
 routes, displaying 689, 1428
 routing table, clearing 676, 1427
 send version 686, 1425
 specifying interfaces 677, 1417
 split horizon 672, 687, 1426
 timers 675, 1420
 version 673, 1421

RMON 470, 807
 alarm, displaying settings 473, 812
 alarm, setting thresholds 471, 808
 commands 807
 event settings, displaying 475, 812
 response to alarm setting 473, 809
 statistics history, collection 475, 810
 statistics history, displaying 477, 812
 statistics, collection 478, 811
 statistics, displaying 479, 813

Routing Information Protocol *See* RIP

routing nformation base, description 1409

routing table, displaying 669, 1409

RSA encryption 344, 345, 858

RSTP 235, 1063
 global settings, configuring 240, 1063
 global settings, displaying 245, 1084
 interface settings, configuring 246, 1071–1082
 interface settings, displaying 250, 1084

running configuration files, displaying 727

S

secure shell 340, 852
 configuration 340, 853

security, general measures 305, 887

serial port, configuring 142, 746

service instance, CFM 510, 512, 1304

sFlow
 flow configuration 185, 815–820
 target device 185, 816

Simple Mail Transfer Protocol *See* SMTP

Simple Network Management Protocol *See* SNMP

single rate three color meter *See* srTCM

SMTP
 event handling 415, 763
 sending log events 415, 763

SNMP 442, 785
 community string 456, 787
 enabling traps 462, 790
 filtering IP addresses 378, 877
 global settings, configuring 444, 787–797
 trap manager 462, 791
 traps, CFM 515, 1317, 1321
 users, configuring 457, 459

SNMPv3 446–464, 793–795
 engine ID 445, 446, 793
 engine identifier, local 445, 446, 793
 engine identifier, remote 446, 793
 groups 451, 794
 local users, configuring 457, 795
 remote users, configuring 459, 795
 user configuration 457, 459, 795
 views 448, 797

SNTP
 setting the system clock 135, 768–770
 specifying servers 137, 769

software
 displaying version 121, 732
 downloading 125, 736
 version, displaying 121, 732

Spanning Tree Protocol *See* STA

specifications, software 1433

srTCM
 police meter 292, 1189
 QoS policy 288, 1189

SSH 340, 852
 authentication retries 343, 855
 configuring 340, 853
 downloading public keys for clients 345, 736
 generating host key pair 344, 858
 server, configuring 342, 856
 timeout 343, 857

SSL, replacing certificate 338

STA 235, 1059
 BPDU filter 249, 1071
 BPDU flooding 241, 247, 1080
 BPDU shutdown 249, 1072
 cisco-prestandard, setting compatibility 1061
 detecting loopbacks 238, 1075
 edge port 248, 251, 1074
 global settings, configuring 240, 1060–1067
 global settings, displaying 245, 1084
 interface settings, configuring 246, 1071–1082
 interface settings, displaying 250, 1084
 link type 248, 251, 1075

- loopback detection 238, 1075
- MSTP interface settings, configuring 257, 1068–1070
- MSTP path cost 257, 1078
- path cost 251, 1065, 1073
- path cost method 242, 1065
- port priority 247, 1080
- port/trunk loopback detection 238, 1075
- protocol migration 249, 1083
- transmission limit 242, 1067
- standards, IEEE 1435
- startup files
 - creating 125, 736
 - displaying 125, 729, 740
 - setting 125, 735
- static addresses, setting 227, 1054
- static routes, configuring 667, 1408
- statistics
 - ARP 666, 1371, 1411
 - ICMP 1371, 1411
 - IP 1371, 1411
 - TCP 1371, 1411
 - UDP 1371, 1411
- statistics, port 162, 983
- STP 240, 1063
 - Also see STA*
- summary, accounting 315, 846
- switch clustering, for management 481, 779
- switch settings
 - restoring 127, 734
 - saving 127, 734
- system clock
 - setting 134, 767
 - setting manually 134, 775
 - setting the time zone 141, 774
 - setting with NTP 138, 770–774
 - setting with SNTP 135, 768–770
- system logs 759
- system software, downloading from server 125, 736

T

- TACACS+
 - logon authentication 308, 834
 - settings 310, 834
- TCN
 - flood 561, 1206
 - general query solicitation 562, 1208
- Telnet
 - configuring 144, 850
 - server, enabling 144, 852
- terminal, configuration settings 755
- TFTP
 - retry count 744
 - timeout 745
- time range, ACL 349, 776
- time zone, setting 141, 774
- time, setting 134, 767
- TPID 210, 1140

- traffic segmentation 187, 1148
 - assigning ports 187, 1148, 1150
 - enabling 187, 1148, 1150
 - sessions, assigning ports 190, 1148, 1150
 - sessions, creating 189, 1148, 1150
- trap manager 93, 462, 791
- troubleshooting 1437, 1439
- trTCM
 - police meter 293, 1192
 - QoS policy 289, 1192
- trunk
 - configuration 168, 993
 - LACP 172, 993, 996
 - load balancing 994
 - static 169, 996
- tunneling unknown VLANs, VLAN trunking 191, 1132
- two rate three color meter *See* trTCM
- Type Length Value
 - See* LLDP TLV

U

- unicast routing 671, 1407
- unidirectional link detection 1047
- unknown unicast storm, threshold 261, 981
- unregistered data flooding, IGMP snooping 562, 1208
- upgrading software 125, 736, 741
- user account 322, 824, 825
- user password 322, 824, 825

V

- VLAN
 - L3 interface, setting type 197
- VLAN trunking 191, 1132
- VLANs 193–223, 1119–1165
 - 802.1Q tunnel mode 214, 1137
 - acceptable frame type 200, 1128
 - adding static members 199, 1129
 - basic information, displaying 1123
 - creating 196, 1126
 - description 193
 - displaying port members 1134
 - displaying port members by interface 202
 - displaying port members by interface range 203
 - displaying port members by VLAN index 201
 - dynamic assignment 331, 896
 - egress mode 199, 1131
 - ingress filtering 200, 1130
 - interface configuration 199, 1128–1132
 - IP subnet-based 219, 1156
 - MAC-based 221, 1158
 - mirroring 223, 1013
 - port members, displaying 1134
 - protocol 215, 1152
 - protocol, configuring 215, 1153, 1154
 - protocol, configuring groups 215, 1153
 - protocol, interface configuration 217, 1154

- protocol, system configuration 215, 1153
- PVID 199, 1131
- tag swapping 224, 1146
- tunneling unknown groups 191, 1132
- voice 299, 1160
- voice VLANs 299, 1160
 - detecting VoIP devices 300, 1160
 - enabling for ports 303, 1163
 - identifying client devices 301, 1162
- VoIP traffic 299, 1160
 - ports, configuring 302, 1163
 - telephony OUI, configuring 301, 1162
 - voice VLAN, configuring 299, 1160
- VoIP, detecting devices 303, 1164

W

- web authentication 324, 908
 - address, re-authenticating 325, 909
 - configuring 324, 908
 - port information, displaying 325, 910
 - ports, configuring 325, 908
 - ports, re-authenticating 325, 909
- web interface
 - access requirements 99
 - configuration buttons 101
 - home page 100
 - menu list 102
 - panel display 101

E052013/ST-R04

ECS4510-28T	149100000189A
ECS4510-28P	149100000189A
ECS4510-28F	149100000189A
ECS4510-52T	149100000191A
ECS4510-52P	149100000191A